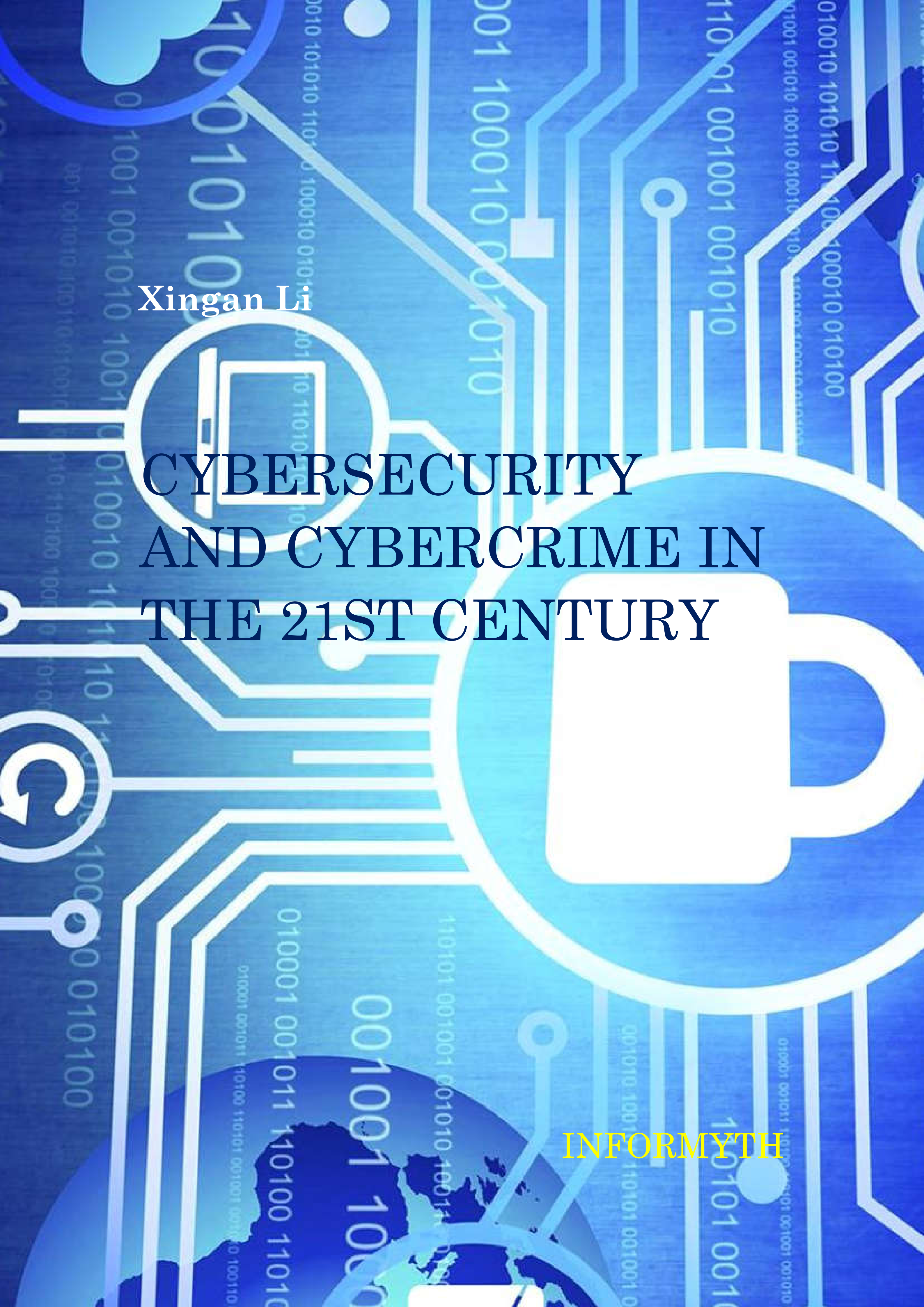


Xingan Li

CYBERSECURITY AND CYBERCRIME IN THE 21ST CENTURY

INFORMYTH

Xingan Li

CYBERSECURITY AND CYBERCRIME

IN THE 21ST CENTURY

INFORMYTH

Made in the Republic of Finland

Valmistettu Suomessa

Title: Cybersecurity and Cybercrime in the 21st Century

First Edition, First Impression, February 2016

1. pianos, Helmikuu 2016

ISBN 978-952-67927-3-6 (PDF)

ISBN 978-952-67927-4-3 (EPUB)

Publisher:

Informyth, Helsinki, Finland

Kustantaja:

Informyth, Helsinki, Suomi

PREFACE

The purpose of this book is to provide a textbook for advanced training course. The content of the book tries to address the challenges posed to legal system by information systems, by clarifying how some significant phenomena stand from the legal viewpoint. Based on the relativity of the concept of cybersecurity, Chapter II analyzes the economic impact of cybersecurity breaches, identifies cybersecurity as a private good that should be provided mainly by the private sector. However, public provision is also necessary when severe security breaches occur and liability mechanisms should be triggered.

In Chapter III, it has been recognized that, while information systems provide modern society with great convenience, it also poses new problems in maintaining social order. One of its negative influences is the anonymity of cyberspace, which makes identity tracing a noteworthy predicament which poses obstacles in detection and investigations. It has been found that cyber anonymity has critical impacts on criminal motivation, and the phenomena of victimization, and should be tackled on different layers including technology and law enforcement. The article explores how the anonymity symbolizes the cyberspace, what threats are posed by cyber anonymity against social order, what potentialities the

anonymity has, how the trans-territorial anonymity was facilitated, and the real impact of anonymity on law and order in the information society.

The purpose of Chapter IV is to present an updated profile of cybercriminality and cybervictimization based on a sample of 115 typical cases prosecuted. The study found that males are responsible for a majority of these cybercrimes. The cybercriminals distribute primarily among the ages between 17 to 45 years old. Domestic perpetrators constitute the absolute majority of the cybercriminals. Outsiders are four times more likely to be involved in cybercrimes than insiders. Most cybercrimes did not involve monetary loss, while the other cybercrimes caused an average of one million dollars of damage. The primarily endangered interests are of private sector. The guardianship of the victims is surprisingly weak, vulnerable to the uncomplicated cybercrimes. The punishments (both imprisonment and fine) against cybercrime are generally light.

Chapter V discusses about cyberstalking. Shortly after traditional stalking had been criminalized, new approaches for stalking emerged as the adoption of some high technological inventions were used in monitoring people's activities. Based on the recognition of stalking as a kind of long-existing human-human observation, this article expatiates on recent development that can be expressed as from traditional stalking to cyberstalking by presenting particular power of information and communications technology and search engines. The article discusses the ambiguous limit between searching and stalking. This article also considers an emerging phenomenon that stalking is being socialized through the pervasion of online social network services.

The purpose of Chapter VI is to explore the legal solutions to unsolicited commercial e-mail. The advantages of e-mail enable it to be one of the most important e-marketing instruments. Spammers are also

motivated by potential profits in spamming. The low costs and high benefits of the spammers, and the high costs and low benefits of the spammed determine the illegal nature of the spamming. The spam poses challenges for e-mail recipients' property rights, fair trade, public morals, cybersecurity, personal data protection, and involves other concerns as well. In dealing with spam, technical and marketing solutions cannot work alone without the legal mechanisms. The legal regulation is justified by balancing the interest between senders, service providers and even users. Criminal sanctions, civil remedies, and international harmonization are alternative steps in establishing legal solutions. As a necessary part of the legislation, punishment for unsolicited commercial e-mails should be more severe. Still, there are a number of limitations to the effectiveness of law enforcement against spamming. Spam must be eliminated by comprehensive mechanisms.

Chapter VII focuses on the extension of victimization of unsolicited messages e-mail with attachments. Based on the analysis of a sample of 501 pieces of unsolicited e-mail messages with attachments, the study finds that e-mail account exposing and seeking can both contribute to victimization; while the receiving of unsolicited messages is just the initial victimization, the reading and reacting to the messages could lead to further victimization of virus attack or financial fraud, and to conspiracy in illegitimate operations such as tax evasion or purchase of falsified documents.

Chapter VIII discusses broadly about cyber warfare. Cyber warfare is increasingly listed alongside nuclear, chemical, and biological weapons as a potential weapon of mass destruction. Interest in and concerns for cyber warfare have also been prevalent for decades. War-oriented writer usually exploited such serious and expensive terms as cyber war, information war, and electronic war to spread their impetuous and cheap ideas. This essay

by no means devaluates serious designs and plans, studies and research, ideas and claims revolving around cyber warfare. Rather, the purpose of this Chapter is to analyze existing jokes, hoaxes and hypes on the so-called cyber warfare, so as to distance serious research from misleading information.

Chapter IX deals with spyware. Spyware poses a substantial menace to security, integrity and confidentiality of information systems. Originating from online commercial advertising strategies, spyware can be used to deceive users, forcibly modify system, and secretly collect information from host computer. Basic consensus can be reached on the definition of spyware upon two factors: unauthorized installation and compromising data. This Chapter puts spyware on a platform of social legal phenomena, giving a review of taxonomy, characteristics, threatened interests and interest group revolving around the standpoints for and against the prohibition of spyware. Upon its appearances, the Chapter takes a look at current legal actions against spyware. To some extent, existing laws provide effective means for combating some specific spyware-related activities.

Chapter X explores into economic approach to cybercrime. The classic economic analysis of crime is limited to handful offences. The application of this approach to cybercrime is one of the efforts in expanding the research field and has significance in designing the framework of legislation and law enforcement. The article analyzes the deterrence from the aspects of probability of detection and severity of punishment. Cybercrime has different characteristics with most traditional offences and challenges some aspects of the previous models and explanations based on the hypothesis of rational offender. The low probability of detection decided by the universality, concealment, complex, expensiveness, and rapid rampancy of cybercrime obstruct the function of

deterrence by punishment. The expected utility of the offender is to a certain extent promoted by the low probability of detection, notwithstanding the punishments in individual cases may be severe. The instauration of cyber police and the implementation of severe punishment leave no marginal deterrence at the current technological level. The ways to improving the deterrence are to adopt techniques to increase probability of detection, conviction, and sentence, and to enhance international legal co-ordination and co-operation to eliminate safe haven.

Finally, Chapter XI concludes the whole book by emphasizing that cybercrimes are different from traditional crimes and thus pose new challenges to the legal systems, and that criminal law plays a necessary but limited role in combating cybercrime. The vulnerabilities should be eliminated by technological means, while the motives should be eliminated by legal instruments.

Keywords: cyberspce, cybersecurity, cybercrime, cyberstalking, cyberwarfare, unsolicited e-mail

Table of Contents

LIST OF FIGURES

LIST OF TABLES

CHAPTER I INTRODUCTION

Insecure cyberspace

Recent decades have witnessed a golden age in social history, previously symbolized by long wars and disasters, but now showing a scene of unparalleled development in information and communications technology (ICT) and related material forms of computers and networks. In both academic and popular discourses, newly-coined words indicate that the information age has arrived and an information society has emerged. The transition eliminated primary obstacles to information accessibility.

As one of the fast increasing fields, Social Networking Services (SNSs) spread in a surprising rhythm into contemporary social life. While the number of users of the SNSs is not available, it was estimated that among Internet users, about 74% of online adults use social networking sites (Pew Research Center 2015). In fact, at present, SNSs are used in a broad range of mobile devices, such as smart phones, cameras, media players, tablets and phablets, and notebook PCs, which are usually connected to the networks when they are in use.

Unfortunately, information systems are likely to crash, and likely to

cause disputes and lawsuits. Furthermore, the order of cyberspace, closely associated with the welfare of citizens, the security of businesses, and the stability of society is, however, becoming increasingly significant, due to increased scale of the online population to over one-sixth of the inhabitants of the globe (for an exploration of social order in cyberspace, see Li 2014, Li 2015). What is problematic in the landscape of the social sciences is that many technological loopholes are constantly being exploited with malicious intent, while technological opportunities are, at the same time, generating various benefits as well. Hence chaos, disorder, social problems, and more severely, crimes pose great threats to the security, reliability, and credibility of the information society.

Cybersecurity has extended its influence into “meat space”, that is, real society, and caused widespread concerns among various entities (Li 2006). Cybercrimes, criminal offences committed by netizens in cyberspace, are new variants of criminal phenomena. This raises many questions as to whether the existing legal system has the capability of deterring cybercrimes.

The development of crime is closely related to social transformation at both the micro and the macro levels. In the temporal dimension, the change of criminal law over time necessitates legal reform, while in the spatial dimension, the difference in criminal laws between the various countries requires international harmonization. As a social phenomenon, crimes change with the development of society. It has previously been recognized that with the advent of ICT, social change brought about by technology is capable of occurring with devastating rapidity.

In order for our society to continue to flourish, legal certainty should be extended to guarantee that criminal activities committed in cyberspace are punished in the physical world.

Structure of this book

After this Introduction, to address the challenges posed to criminal law by information systems, it is necessary to clarify how the phenomenon stands from the legal viewpoint. Based on the relativity of the concept of cybersecurity, Chapter II analyzes the economic impact of cybersecurity breaches, identifies cybersecurity as aprivate good that should be provided mainly by the private sector. However, public provision is also necessary when severe security breaches occur and liability mechanisms should be triggered.

In Chapter III, it has been recognized that, while information systems provide modern society with great convenience, it also poses new problems in maintaining social order. One of its negative influences is the anonymity of cyberspace, which makes identity tracing a noteworthy predicament which poses obstacles in detection and investigations. It has been found that cyber anonymity has critical impacts on criminal motivation, and the phenomena of victimization, and should be tackled on different layers including technology and law enforcement. The article explores how the anonymity symbolizes the cyberspace, what threats are posed by cyber anonymity against social order, what potentialities the anonymity has, how the trans-territorial anonymity was facilitated, and the real impact of anonymity on law and order in the information society.

The purpose of Chapter IV is to present an updated profile of cybercriminality and cybervictimization based on practical materials. The study used a sample of 115 typical cases prosecuted (during 18 March 1998 to 12 May 2006), published officially on the web site of the United States Department of Justice. The study found that males are responsible

for a majority of these cybercrimes. The cybercriminals distribute primarily among the ages between 17 to 45 years old. Domestic perpetrators constitute the absolute majority of the cybercriminals. Outsiders are four times more likely to be involved in cybercrimes than insiders. Most cybercrimes did not involve monetary loss, while the other cybercrimes caused an average of one million dollars of damage. The primarily endangered interests are of private sector. The guardianship of the victims is surprisingly weak, vulnerable to the uncomplicated cybercrimes. The punishments (both imprisonment and fine) against cybercrime are generally light.

Chapter V discusses about cyberstalking. Shortly after traditional stalking had been criminalized, new approaches for stalking emerged as the adoption of some high technological inventions were used in monitoring people’s activities. Based on the recognition of stalking as a kind of long-existing human-human observation, this article expatiates on recent development that can be expressed as from traditional stalking to cyberstalking by presenting particular power of information and communications technology and search engines. The article discusses the ambiguous limit between searching and stalking. This article also considers an emerging phenomenon that stalking is being socialized through the pervasion of online social network services.

The purpose of Chapter VI is to explore the legal solutions to unsolicited commercial e-mail. The advantages of e-mail enable it to be one of the most important e-marketing instruments. Spammers are also motivated by potential profits in spamming. The low costs and high benefits of the spammers, and the high costs and low benefits of the spammed determine the illegal nature of the spamming. The spam poses challenges for e-mail recipients' property rights, fair trade, public morals, cybersecurity, personal data protection, and involves other concerns as

well. In dealing with spam, technical and marketing solutions cannot work alone without the legal mechanisms. The legal regulation is justified by balancing the interest between senders, service providers and even users. Criminal sanctions, civil remedies, and international harmonization are alternative steps in establishing legal solutions. As a necessary part of the legislation, punishment for unsolicited commercial e-mails should be more severe. Still, there are a number of limitations to the effectiveness of law enforcement against spamming. Spam must be eliminated by comprehensive mechanisms.

Chapter VII focuses on the extension of victimization of unsolicited messages e-mail with attachments. Based on the analysis of a sample of 501 pieces of unsolicited e-mail messages with attachments, the study finds that e-mail account exposing and seeking can both contribute to victimization; while the receiving of unsolicited messages is just the initial victimization, the reading and reacting to the messages could lead to further victimization of virus attack or financial fraud, and to conspiracy in illegitimate operations such as tax evasion or purchase of falsified documents.

Chapter VIII discusses broadly about cyber warfare. Cyber warfare is increasingly listed alongside nuclear, chemical, and biological weapons as a potential weapon of mass destruction. Interest in and concerns for cyber warfare have also been prevalent for decades. War-oriented writer usually exploited such serious and expensive terms as cyber war, information war, and electronic war to spread their impetuous and cheap ideas. This essay by no means devaluates serious designs and plans, studies and research, ideas and claims revolving around cyber warfare. Rather, the purpose of this Chapter is to analyze existing jokes, hoaxes and hypes on the so-called cyber warfare, so as to distance serious research from misleading information.

Chapter IX deals with spyware. Spyware poses a substantial menace to security, integrity and confidentiality of information systems. Originating from online commercial advertising strategies, spyware can be used to deceive users, forcibly modify system, and secretly collect information from host computer. Basic consensus can be reached on the definition of spyware upon two factors: unauthorized installation and compromising data. This Chapter puts spyware on a platform of social legal phenomena, giving a review of taxonomy, characteristics, threatened interests and interest group revolving around the standpoints for and against the prohibition of spyware. Upon its appearances, the Chapter takes a look at current legal actions against spyware. To some extent, existing laws provide effective means for combating some specific spyware-related activities.

Chapter X explores into economic approach to cybercrime. Modern economic approach to crime seeks to observe criminal behaviour in the light of pure economic factors. While abundant literatures address the issue, the economic dimension of crime is an underdeveloped perspective. The classic economic analysis of crime is limited to handful offences. The application of this approach to cybercrime is one of the efforts in expanding the research field and has significance in designing the framework of legislation and law enforcement. The article analyzes the deterrence from the aspects of probability of detection and severity of punishment. Cybercrime has different characteristics with most traditional offences and challenges some aspects of the previous models and explanations based on the hypothesis of rational offender. The low probability of detection decided by the universality, concealment, complex, expensiveness, and rapid rampancy of cybercrime obstruct the function of deterrence by punishment. The expected utility of the offender is to a certain extent promoted by the low probability of detection,

notwithstanding the punishments in individual cases may be severe. The instauration of cyber police and the implementation of severe punishment leave no marginal deterrence at the current technological level. The ways to improving the deterrence are to adopt techniques to increase probability of detection, conviction, and sentence, and to enhance international legal co-ordination and co-operation to eliminate safe haven.

Finally, Chapter XI concludes the whole book by emphasizing that cybercrimes are different from traditional crimes and thus pose new challenges to the legal systems, and that criminal law plays a necessary but limited role in combating cybercrime. With the routinization of the phenomenon of cybercrime, criminal-law reform will slow down. Overall, solutions should be found from the impacts of vulnerabilities and motives. The vulnerabilities should be eliminated by technological means, while the motives should be eliminated by legal instruments.

References

1. Internetworldstats.com. 2015. Internet Usage Statistics-The Big Picture. Retrieved 15 February 2016, from http://www.internetworldstats.com/stats.htm.
2. Li, X. 2006. Cybersecurity as a Relative Concept. *Information & Security: An International Journal*, 18, pp. 11−24.
3. Li, X. 2014. Exploring into regulatory mode for social order in cyberspace. *Webology*, 11 (2), 1−8.
4. Li, X. 2015. Cyberspace and the Informed Rationality of Law. *The Romanian Journal of Sociology*, 26, pp. 3−27.
5. Pew Research Center. (2015). Social Networking Fact Sheet. Retrieved 15 February 2016, from

http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/

CHAPTER II CYBERSECURITY AS A RELATIVE CONCEPT

Introduction

The Internet has become a critical infrastructure for both public and private sectors and has brought new levels of productivity, convenience, and efficiency. The increasing incidents of Internet attacks representing examples of how vulnerable the information systems are, how far the offensive technology outpaces the defensive technology, how easy various malicious programs are created and how smart they can spread all over the Internet rapidly, have started to impact the practical facets of our lives. At the same time, the attackers are able to conceal their attacks by disabling logging facilities or modifying event logs, so their activity goes undetected. Even worse, some automated programs have been designed to specifically disable anti-virus software or penetrate firewalls. The security violations have multi-dimensional impacts on both consumers and businesses, including time, human resources, monetary losses and psychological losses.

The Internet and the larger information infrastructure are not secure

(National Research Council 1996). McCormick identified five reasons why Internet is vulnerable: failing to enforce policies, ignoring new vulnerabilities, relying too much on technology, failing to thoroughly investigate job candidates, and expecting too much from technical skills (McComick 2005). These risks cause serious insecurity problems in the information society (Farmer 1996).

While the governments have made efforts to better secure their own computer networks to prevent terrorists from hacking into computer systems, the governments have been increasingly concerned that the private sector is vulnerable to cyberterrorism. The question being asked is whether private businesses provide enough cybersecurity, or some form of government involvement is justified. Many empirical studies examined the economic impact of cybersecurity breaches. Theories diversify in regarding the cybersecurity as an externality (Chandler 2004), a public good (Coyne and Leesen 2005), or a private good (Powell 2001).

Based on the concept of relative cybersecurity, this Chapter analyzes the economic impact of cybersecurity breaches, whether cybersecurity is a public good or a private good. It also establishes liability mechanism for cybersecurity breaches.

Impact of Cybersecurity Breaches

Increasing Investment of Users in Cybersecurity

The users' investment in cybersecurity takes on the tendency of increasing. Although exact statistics on these expenditures is unavailable, the add-up

of global users' financial costs will reach a surprising figure. According to a survey conducted by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI), nearly all of the companies surveyed in 2005 used anti-virus software, firewall, and some measures of access control. Besides the hardware and software, the organizational users also have to employ security personnel or institutions to maintain their systems. These measures induce the increase of the investment of network users. But in fact, security measures can hardly ever be a perfect assurance against damage and accidents. Absolute security becomes too expensive to be reasonable (Daler, Gulbrandsen, Melgrd, and Sjølstad 1989, p. 15).

Frequent Occurrence of Cybersecurity Breaches

Although the investment in cybersecurity is increasing year by year, the breaches still occur frequently. The potential for information security breaches, as well as the magnitude of potential losses associated with such breaches, has been confirmed by empirical studies.

The annual surveys on information security breaches have pointed out that cybersecurity breaches are ubiquitous. The 2005 survey conducted by CSI and FBI revealed that 56 percent of the surveyed 693 U.S. computer security practitioners acknowledged unauthorized use of a computer in their organization in the last 12 months (Gordon, Loeb, Lucyshyn, and Richasrdson 2005, p. 11).

CERT Coordination Center reported that the computer security vulnerabilities increased nearly 35-fold during one decade with 171 separate holes reported in 1995 and 5,990 reported in 2005 (CERT Coordination Center 2005). In the recent years, the publicly disclosed

virus attacks are billing the global computer users in an accelerated speed, even though many of the users are unaware of, or unwilling to report the losses.

Increasing Costs of Cybersecurity Breaches

As a consequence of the frequent occurrence of cybersecurity breaches, the losses of these breaches are increasing as well. The losses can be divided into direct and indirect, tangible and intangible, and short-term and long-term. Neumann stated that costs of cybercrime are difficult to measure; however, these costs are reasonably substantial and growing rapidly (Neumann 1999). Scholars proposed various models to try to measure the costs of security breaches, such as in the Forrester Research. Howe and colleagues' analysis indicated that, if the perpetrators were to unlawfully transfer $1 million from an online bank, the financial influence to the bank would reach $106 million (Howe, McCarthy, Buss, and Davis 1998).

The direct losses are those directly involved in the attacks, including interruption of business, destruction of software and hardware, expenditure on recovering the systems, installation and update of security means, recruiting security personnel, etc. The indirect losses are losses indirectly related to the attacks, such as reduction of consumers, decrease of stock prices, etc. The other kinds of losses are also easy to emerge.

The 2005 CSI/FBI survey noted that, of the 639 respondents that were willing and/or able to estimate losses due to security breaches, such breaches resulted in losses close to $130 million (Gordon, Loeb, Lucyshyn, and Richasrdson 2005, p. 15). On the other hand, Lukasik claims that cybercrime costs are essentially doubling each year (Lukasik 2000). The problem becomes even more complex when one considers the "black figure"

of these crimes. Ullman and Ferrera mentioned that, according to FBI estimates, only 17 percent of computer crimes are reported to government authorities (Ullman and Ferrera 1998).

Relativity of the Cybersecurity Concept

There are various answers to the question "What is cybersecurity?" Cybersecurity is a comparative concept. On one hand, it includes the comparison between security and attack techniques. On the other hand, it includes comparison between different security techniques and measures. Considering the comparison between the techniques for security and attack, it is publicly well recognized that the attack techniques develop faster than the security techniques, regardless of the reasons. In other words, the hardware, the software, or the other information system components are always vulnerable and this fact can be exploited. We could call this the absolute level of security. Considering the comparison between the different security techniques, the existence of different environments, the possession of different hardware, software and other equipment, and the adoption of different security techniques, all this leads to difference in the level of security. Therefore, each of the individual or organizational users has a different security level.

Some viewpoints regard cybersecurity as an externality (Camp and Wolfram 2000, pp. 31-39). Camp and Wolfram point out that if a company does a poor job at cybersecurity, other companies may be affected negatively. Thus, the cost is an externality to the owner of the infected machine (ibid.). However, if we identify cybersecurity as an externality, it is inevitable that to the extent investments in computer security create positive externalities, too little will be provided.

Security is not the reason that drives the attackers to violate security and launch attacks, nor the condition that facilitates the attacks, but the target that the attacks aim at. In fact, there is no clear boundary between security and insecurity. Security and insecurity have only quantitative difference, but no quality distinction. Neither absolute security nor complete insecurity exists. That is to say, security and insecurity should be considered as security between zero percent and 100 percent. Therefore, security is a relative concept. The security of a higher level is security, while the security of a lower level is insecurity.

Although the information systems on the Internet all have a similar framework, they lack any central control system and are uncontrollable. Not only the physical system, but also the operational process is uncontrollable. Thus, to a great extent, the security of the Internet depends on the security measures taken by the end users, either individuals or organizations. However, the security measures of individual and organizational users are widely different due to the difference in hardware, software, and human resources.

The level of security of the end users on the network is different; an absolute value of security does not exist. Security is just a comparison of relative values. It is both the result of comparison between users and the comparison between past and present, i.e., horizontal and vertical comparison. Due to the large number of network users and the rapid change in the network environment, the result of this comparison changes constantly. In general, a higher level security will change quickly into a lower level security (insecurity) with transformation of techniques and the environment. Therefore, the cybersecurity measures have to be updated and renewed timely, frequently, and efficiently.

If the cybersecurity measures cannot be updated and renewed in a timely, frequent and efficient manner, vulnerabilities might occur.

Vulnerability is not the security or insecurity themselves, but a factor that makes it impossible to realize perfect security, and an extra loophole caused by the external factors in the investor's production of the expected complete security. It is the natural adversary of the security product, i.e., flaws that can be detected and exploited by the potential attackers to commit harm and cause loss.

Table 1 Classical division of goods in economy

Classic division of goods in economy		Exclusion from consumption	
		YES	NO
Competition in consumption	YES	private good: food, clothing, toys, furniture, cars	common good: natural environment
	NO	club good: private schools, cinemas, clubs,	public good: national security (army and police forces)

Source: Wikipedia, at http://en.wikipedia.org/wiki/Good_%28economics%29.

Provision of Cybersecurity as a Private Good

In economics, goods are traditionally classified into four categories as listed in Table 1. Besides other issues, private good and public good can be generally regarded as a pair of opposites. The main features of the private good are excludability and rivalry.

According to Samuelson (1954), public good is a good that produces a positive externality and which is characterized by non-rival consumption

and non-excludability. The private provision of private goods, or public provision of public goods are not the unique ways in providing these two kinds of goods (let us not consider the other kinds of goods here). The ways of provision of these two kinds of goods can be illustrated as shown in Table 2.

Table 2 Ways of provision of private goods and public goods

Different ways of provision of different goods	Private provision	Government provision	Mixed Provision
Private goods	clothes, food, car, private housing	food supply as in communist China in end 1950s	transportation, medical care
Public goods	foreign aid	national defence	pollution reduction

The public good is usually confronted with the problem of being underprovided or not being provided when it is put on the private market. Such a problem appears in providing cybersecurity. Generally, a higher level of cybersecurity would benefit both the individual or organizational owner and users other than the owner. Because insecure computers are vulnerable to be manipulated to launch attacks against other computers, it is reasonable to assume that if an owner maintains a higher level of cybersecurity, the other users' computers may experience a lesser risk of being attacked.

Then the other users would have the good reason to reduce their investment in security protection. The computer users' security provision

only diminishes the probability of the others' computers being attacked. However, since individuals are not generally liable for the damage caused when a hacker uses their computer, they do not benefit from the increased security (Varian 2002). And because users with ability to provide security do not benefit, they will fail to provide it. The same applies to other computer owners, and, therefore, everybody is in a worse situation than would be if everyone provided the security that would have spillover benefits for everyone else.

As we have seen, cybersecurity is both excludable and rivalrous. Cybersecurity has neither territorial boundary nor industrial limit. In the global village, all individuals and organizations are confronted with risks of the same level. In this environment, the security of individuals or organizations' systems matters firstly to themselves. Only in some accidental situations are others involved, such as in the case of DOS attacks.

Powell provides evidence from the financial services industry to prove that cybersecurity is hardly a public good (Powell 2001). Individuals and organizations have excludability in cybersecurity. The excludability of cybersecurity roots in the three characteristics of cybersecurity, i.e., confidentiality, integrity and availability, among which confidentiality fully expresses the excludability of cybersecurity. We could see the situation this way: if security is available to one user, it is unavailable to other users, and if others enjoy security, ones' security does not exist any longer. Unsurprisingly, cybersecurity is characterized as preservation of confidentiality, ensuring that information is accessible only to those authorized to have access; integrity, safeguarding the accuracy and completeness of information and processing methods; availability, ensuring that authorized users have access to information and associated assets when required. The users' security is enjoyed solely by themselves.

Any sharing entails that systems become insecure. In fact, hackers are precisely the exploiters and sharers of insecure systems. Therefore, cybersecurity has more excludability than any private good.

On the other hand, the cost of expanding security to others is not zero, but enormously high. If one user enjoys a higher level of security, the level of security of the others will relatively decrease. As mentioned above, there is no perfect security. Security and insecurity are relative concepts that exist in comparisons. If one enjoys a higher level of cybersecurity, the level of security of the others will decrease to insecurity. The competition between the security measures is the reason that causes increase of the difference between the relative securities. Of course, the enhancement of the total security level benefits from that competition.

Katyal's study stresses that to some extent private security measures may increase crime (Katyal 2005). The basic assumption behind this argument is that, if one household locks its door, the thief will turn to the neighbor whose doors are left unlocked. Therefore, locking of one's own door breaks the reciprocity and mutual trust in the neighborhood. If we consider the fact that currently nearly all households, companies, and even government agencies "lock their own doors," we can easily conclude that this assumption is absurd. Only when every household, company and governmental agency is convinced not to take such "inefficient" measures is such an assumption significant. The author believes that such an assumption ignores the dual value of locking in the prevention of crime: on one hand, locking protects from damage and harm, making the potential criminals shrink back at the sight, or taking criminals more time before suffering losses; on the other hand, locking increases the potential criminals' time consumption and material costs in looking for new victims, and even making it impossible for them to find one. If none of the households and organizations locks their doors, potential criminals can

easily find possible targets. Therefore, the difficulty of crime will decrease, and the efficiency will increase. The potential criminals are indifferent about costs, benefits, likelihood of success.

This pertains particularly to cybersecurity. If every computer owner is encouraged not to use security control, the computer will be more vulnerable to attacks. Assuming that the environment and the potential of all individual and organizations' computers are the same and the risk of being attacked is also approximately similar, then only when the benefits related to cybersecurity are equal could the provision of public cybersecurity be efficient. But this situation rarely exists in reality. Therefore, an unlimited public cybersecurity would be excessive for some individuals and organizations and insufficient for others. The situation of abundance is economically inefficient, while the situation of insufficiency is inefficient in terms of security. Hence, both ways, the public cybersecurity control cannot function optimally. In result, if cybersecurity is provided in the mode of public good, it is impossible to be more beneficial than as a private good.

Kobayashi notes that cybersecurity is different from traditional security (Kobayashi 2005). To discourage crime ex ante in the general criminal context, the government could implement sufficient level of punishment to deter the crime from accruing. In the case of cybercrime, the likelihood of detecting is so low that the penalty imposed would have to be of considerable magnitude to deter cybercrime. In what follows, the author will explore the possibility of establishing liability for the different participants in the process of cybersecurity provision.

Public Provision of Cybersecurity: Liability Mechanisms

Even if it were technically feasible to keep all systems 100% secure, the costs would have been so prohibitive as to render such an approach an economic prescription for disaster. The government can neither provide cybersecurity nor manipulate the systems. Naturally, one of the Ernst & Young survey's key findings was that only 11% deemed government security-driven regulations as being highly effective in improving their information security posture or in reducing data protection risks (Earnest & Young 2004). However, any argument stating that the governments can play no role in the field of cybersecurity is over skeptical. The governments can play a necessary role in deterring the attackers, but they are by no means helpless in the maintenance of an adequate level of cybersecurity. Their roles are to impose penalty through legislation and deter crime by means of ex post law enforcement. Providing cybersecurity as a public good is confronted with greater difficulties in international cooperation than as a private good. Even if some countries can convince their taxpayers to pay for the expenses involved in the public provision of cybersecurity, if you cannot simultaneously convince all countries to do so, it will not be cost-efficient. In this section, the author will analyze the characteristics of the possible liability of various players in the field of cybersecurity.

Liability of Hackers

Ballon argues that the major benefits of holding the hacker liable for the damage he causes is that the target has more choices and control in applying the law against hackers (Ballon 1997). Compared to a criminal action, the liability of hackers can be justified by that it grants the

plaintiff “greater control over the litigation and potentially better long-term relief;” that it encourages attack reporting (Gripman 1997); and that a target will have the motive to recover losses at the same time of punishing the perpetrator (Hatcher, McDannel and Ostfeld 1999).

The disadvantage of tort liability of hackers lies in two aspects: on one hand, the plaintiff has to pay a significant amount of money before receiving any compensation; on the other hand, most hackers have had and will have greater incentives to be judgment-proof (Brooke 2000). If a hacker has little to lose under tort liability mechanism, his most rational choice will be to hide more secretly himself and his assets (Calkins 2000). In the networked world, tracking a hacker or finding his money will need more energy, time, and costs, and will even prove to be an impossible task. As a result, the hacker would carry out the act more judgment-proof. Even worse, the hacker might be forced by the civil actions to commit other money-harvesting offences to support his actions.

Currently, dozens of countries have enacted domestic law against cybercrime. In addition, there have also been successful international legal actions, such as the Convention on Cybercrime (2001) and other domestic provisions. Although the legislation is already there, the practical effects are doubtful. There are many hackers but the detection probability is quite low and the application of legislation is rare.

Liability of Internet Service Providers

Internet Service Providers (ISP)’s tort liability plays an important role in the following two cases: first, a lower level of ISP’s security standard might be exploited by hackers; and second, the ISP’s vicarious liability for its employee’s security breach makes it easier to recover the target’s losses

(Icove, Seger, and VonStorch 1995, p. 427). To justify the first aspect, an important economic consideration is that the ISP's cost to improve its security level is lower compared to the hackers' high potential cost to society, and with the security standard the security condition becomes more certain and reliable (Icove, Seger, and VonStorch 1995). This would be expected to lower the overall cost of the Internet service, provide incentive for Internet participation, and increase the value of the network to society (Goodman 1997). There is no theoretical obstacle in applying the tort liability to cybersecurity breaches.

The only problems in applying tort liability to all ISPs is that there is no uniform standard; that it would be difficult to provide such a standard; and that dual or multiple standard would surely motivate some ISPs to maintain a lower level of security due to economic reasons. The result of this dilemma will be that no deterrence functions on hackers.

Liability of Security Problems Publishers

The security (holes) publisher has two aspects of gain from the publication, one is that the publication can prevent some harm suffered by the general public, the other is that the publication realises more economic or other benefits. However, it takes great risk resulting in users' losses in case hackers exploit the publicized loopholes. In addition, the users have to invest in improving their security protection when they know the new publicized loopholes.

According to Coarse's general principle (Coase 1960), whether the publisher should be held liable for his publication is a question of whether the gain of both the general public users from stopping the potential harm and the publisher himself from obtaining a higher confidence value is

greater than the losses that the users suffer from the attacks launched exploiting the publicized loopholes and from the extra investment in preventing such attacks. In different cases, the cost effectiveness is different, and is hard to prove. Finally, as Preston and Lefton put it:

The question is not whether an individual publication causes more harm than good; it is whether a particular rule of liability governing computer security publications causes more harm than good (Preston, and Lofton 2002, p. 130).

Liability of Security Providers

The rapid growth of the computer security industry leads people to consider whether security providers should be held liable when their products and services fail to protect against hackers. Developing higher security level of products and providing high security level of services are costly, but work to prevent hacking from taking place.

Security providers' liability will create incentives for them to provide products or services of at least a standard level. The products and services containing security holes take great risks of product liability if their advertisements stated that they are "hack-proof" (Drummond and McClendon).

The problem with holding security providers liable is that goods and services are usually provided subject to contract or licensing agreements, making tort liability inappropriate because the parties have bargained to allocate the risk between them (Perle, Fischer, and Williams 2000).

The reasonable way in which the agreements are concluded is that neither of the two parties wants to bear more risk. But in general, the

party of product or service users might have the greater discretion in choosing with more guarantees and less expenses. The security providers will be generally worse-off.

Liability of Software Vendors

Most of the security holes come from the bad design of software (and sometimes hardware). The software vendors control the only key to solve this problem through fixing their software. However, this work also consumes human resources and investments in terms of money. Therefore, vendors generally do not have the incentive to do so. A way to incorporate their better work into their best interests is to raise the risk of liability, which will raise the cost of their products. If software vendors have liability costs, they will pass those on to users. In turn, the vendors might as well pay to fix the problems.

Liability of Software Authors

Since the authors of software (the programmers) have the biggest opportunity to prevent problems, it seems appropriate to focus on making them responsible for the security of their products (Fisk 2002). Nonetheless, there are some unique aspects of computer software that make it challenging to apply traditional notions of product liability.

Under such circumstances, if we impose liability on the authors, it is impossible, because the author gets no income to pay the compensation; it is inefficient, because the author would be discouraged from contributing; and it is also unfair, because the users use the software for free and

voluntarily.

Liability of System Owners

Systems can be both targets and tools in attacks. For example in a Distributed Denial of Service attack, the attacks are launched from numerous manipulated computers. The owners of such systems, who use software written and sold by third parties, cannot fully secure their systems, cannot stop unforeseeable outsiders' exploitation, and have no way to reduce the risks. In order to hold the system owners liable, two prerequisites are necessary to be in place: the establishment of a security standard, and the mechanism of insurance. The latter was discussed by Fisk in analogy to vehicle operators who are often legally required to carry insurance against accidents (Fisk 2002).

Conclusion

This Chapter argues that cybersecurity is a private good and should be provided mainly by the private sector. Regarding cybersecurity as a public good would discourage the private sector to invest in security provision. From this standpoint, an early government intervention would reduce the effectiveness and efficiency of cybersecurity.

However, in terms of prevention of security breaches, law enforcement can play an important role in establishing and enforcing liability mechanisms. Although it is still controversial whether and how cybersecurity players should be held liable for their activities, every step

made in this direction will bring benefits to the private sector to achieve their goals.

References

1. Ballon, I. C. Alternative Corporate Responses to Internet Data Theft, in 17th Annual Institute on Computer Law 737, 744 (PLI Patents, Copyrights, Trademarks & Literary Prop. Course, Handbook Series No. 471, 1997).
2. Brooke, J. 2000. Calm Scene Isn't Really. Police Say, *New York Times*, 22 April 2000, C1.
3. Calkins, M. M. 2000. They Shoot Trojan Horses, Don't They? An Economic Analysis of AntiHacking Regulatory Models. *Georgia Law Journal*, vol. 89, no. 171, pp. 214 217.
4. Camp, L. J., and Wolfram, C. 2000. Pricing Security, in Proceedings of the CERT Information Survivability Workshop (Boston, Massachusetts, 24-26 October 2000), pp. 31-39.
5. CERT Coordination Center, CERT/CC Statistics 1988-2005 (2005), <http://www.cert.org/stats/cert_stats.html> (14 Dec. 2005).
6. Chandler, J. A. 2004. Security in Cyberspace: Combating Distributed Denial of Service Attacks. *University of Ottawa Law & Technology Journal*, vol. 1 (2003-2004): pp. 231-261.
7. Coase, R. H. 1960. The Problem of Social Cost. *Journal of Law and Economics*, vol. 3, pp. 1-44.
8. Coyne, C., and Leeson, P. 2004.Who Protects Cyberspace? Working

Paper 24, George Mason University, Department of Economics, Global Prosperity Initiative.

9. Daler, T., Gulbrandsen, R., Melgrd, B., and Sjølstad, T. 1989. *Security of Information and Data.* Ellis Horwood.

10. Drummond, N., and McClendon, D. J.2001. Cybercrime – Alternative Models for Dealing with Unauthorized Use and Abuse of Computer Networks, (Summer 2001), <http://gsulaw.gsu.edu/lawand/papers/su01/drummond_mcclendon/> (14 Dec. 2005).

11. Earnest & Young, Global Information Security Survey 2004, BYG No. FF0231, <http://www.ey.com/global/download.nsf/International/2004_Global_Information_S curity_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf> (14 Dec. 2005).

12. Farmer, D. 1996. Shall We Dust Moscow?: Security Survey of Key Internet Hosts & Various Semi-Relevant Reflections, November-December 1996, <http://www.trouble.org/survey/> (14 Dec. 2005).

13. Fisk, M. 2002. Causes and Remedies for Social Acceptance of Network Insecurity. Paper presented at Workshop on Economics and Internet Security, University of California, Berkeley, 16-17 May 2002.

14. Goodman, M. D. 1997. Why the Police Don't Care about Computer Crime. *Harvard Journal of Law and Technology*, vol. 10, no. 3, pp. 465-494.

15. Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. 2005. *Tenth Annual CSI/FBI Computer Crime and Security Survey* (Computer Security Institute, 2005).

16. Gripman, D. L. 1997. The Doors Are Locked but the Thieves and Vandals Are Still Getting in: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem. *J. Marshall J. Computer & Information Law*, vol. 16, no. 167, pp. 174-176.

17. Hatcher, M., McDannel, J., and Ostfeld, S. 1999. *Computer Crimes.* American Criminal Law Review, no. 36.

18. Howe, C., McCarthy, J. C., Buss, T., and Davis, A. 1998. *The Forrester Report: Economics of Security*.

19. Icove, D., Seger, K., and VonStorch, W. 19995. *Computer Crime: A Crimefighter's Handbook*, O'Reilly and Associates, Inc.

20. Katyal, N. K. 2005. The Dark Side of Private Ordering for Cybersecurity, in *The Law and Economics of Cybersecurity*, ed. Mark F. Grady and Francesco Parisi (Cambridge University Press, November 2005).

21. Kobayashi, B. H. 2005. An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and Other Pubic Security Goods, *Supreme Court Economic Review*, no. 14.

22. Lukasik, S. J. 2000. Protecting the Global Information Commons. *Telecommunication Policy*, vol. 24, nos. 6-7, pp. 519-531.

23. McCormick, J. 2005. Five Reasons You're not Secure, 5 April 2005, <insight.zdnet.co.uk/internet/security/0,39020457,39193819,00.htm > (14 Dec. 2005).

24. National Research Council. 1996. *Cryptography's Role in Securing the Information Society*. Washington, DC: National Academy Press.

25. Neumann, P. G. 1999. Information System Adversities and Risks, paper presented at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Stanford, CA: Hoover

Institution.

26. Perle, E. G., Fischer, M. A., and Williams, J. T. 2000. Electronic Publishing and Software. Part A, Computer Law (January 2000).

27. Powell, B. 2001. Is Cybersecurity a Public Good? Evidence from the Financial Services Industry, Working Paper Number 57 (The Independent Institute, 15 March 2001).

28. Preston, E. M., and Lofton, J. 2002. Computer Security Publications: Information Economics, Shifting Liability and the First Amendment. *Whither Law Review*, vol. 24, no. 71.

29. Samuelson, P. A. 1954. The Pure Theory of Public Expenditure. *Review of Economics and Statistics*, no.36, pp. 387-389.

30. Ullman, R. L., and Ferrera, D. L. 1998. Crime on the Internet. *Boston Bar Journal*, no. 6.

31. Varian, H. R. 2002. System Reliability and Free Riding, in Proceedings of the First Workshop on Economics and Information Security (University of California, Berkeley, 16-17 May 2002).

CHAPTER III IMPACT OF ANONYMITY ON CYBERSECURITY

Introduction

The pervasion of information systems facilitates efficient access to information. While privacy is at high risk, anonymity, invisibility, and concealment of criminal traces become issues of broad concerns. The anonymity of cyberspace makes identity tracing a noteworthy predicament which poses obstacles in detection and investigations. This Chapter deals with the formation and problem of anonymity in cyberspace in general, and anonymity of cybercriminals in particular. It has been found that cyber anonymity has critical impacts on criminal motivation, and the phenomena of victimization, and should be tackled on different layers including technology and law enforcement.

Following this section, the Chapter will explore how the anonymity symbolizes the cyberspace, what threats are posed by cyber anonymity against social order, how the anonymity protects cybercriminals, how the trans-territorial anonymity was facilitated, and the real impact of anonymity on law and order in the information society.

Wrestling between Cyber Anonymity and Law and Order

Information systems have been increasingly critical in facilitating efficient access to information. Today, approximately 3 billion users, or 42% of the world population (Internet World Stats 2014) entered a new space networked by instant transfer of information. With much more information being accumulated, consumption of information becomes a double-edged process. While there is superfluous spam information, privacy is at high risk. Although people have appreciated the value and significance of cyber anonymity, negative concerns also emerge in anonymity, invisibility, and concealment of criminal traces. Cybercrime differs from traditional crimes in many different ways, including its universality and complexities, in particular, its anonymity, concealment, and invisibilities. The anonymity of cyberspace makes identity tracing a noteworthy predicament which poses obstacles in detection and investigations.

For example, in the case of spam, the e-mail can be both the instrument and the objective that are used in commercial, political, malicious, or illegal schemes. As a marketing and communications means, e-mail has been gradually abused. Unsolicited commercial mails (UCE) are typically sent anonymously or with a fabricated identity, and the recipients cannot discontinue successive messages. Messages of this kind furthermore consist of false or misleading headers, deceiving recipients to retrieve messages that they do not desire. Moreover, the recipients have no technique of expressing their inclination not to receive such messages, and have no approach of requesting compensation even if they undergo

loss. The abuse of e-mail has turned into a public annoyance in the online background. Even if the application of anti-spam services and technologies is escalating, the degree of spam is continuing to boost as swift (OECD 2004, pp. 2-3; OECD 2005, p. 6), becoming a predicament not only for individual e-mail accounts, but also for business accounts.

Another example is cyber terrorism. Despite the fact that cyber terrorism has not developed into a reality as lots of people worried at the end of 20th century, it becomes a gorgeous preference for modern-day terrorists for a number of reasons (Weimann 2004, p. 6). It is cheaper, more anonymous, aiming at a more massive target and number of targets, distantly conducted, and affecting a larger number of people globally. International society has barely implemented any countermeasures against conventional terrorism in the last few years. Weimann claimed that terrorism in cyberspace was more anonymous than conventional terrorist schemes. The fact that terrorists could exploit "screen names" or log on as a "guest user" makes it very difficult for security agencies and police forces to track down their real identity. What made it worse were that in cyberspace there were no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart (ibid., p. 6), making terrorists specially unidentified.

Maybe the most real threats and the most serious worries come from offences such as harassment and murder. In offences where information systems are used as means of committing verbal assault, threat, harassment, alarming, spam and fraud, the motivation of the perpetrator is to harass and to kill the victim. The function of the Internet as a means of communications and with a high anonymity of interaction often entraps the victims into unforeseeable dangers. In 2005, China Ministry of Public Security investigated 1,000 assassination cases, in many of which the criminals found the potential victims through the Internet (Yi 2006). In

many criminal cases, stalkers and murderers find, follow, entice, and intimidate victims through the communication and interaction of various Internet services, usually anonymously.

On the other hand, concerning the legal status of cyber anonymity, people have long been disputing in vain. Conventional countermeasures and theories about crime prevention were based on its material influence and on the material environment, although non-material factors have long existed, too. Activities in information systems can be expressed in a physically invisible form. What are physically visible in information systems are those physical existences, such as hosts and terminals, displayers, keyboards, mouse, and cables, while the mechanisms by which the computers function are invisible. Cyberspace is developed from information systems as an abstract space, differing from the material devices of information systems that include terminals and cables. It is invisible and intangible if compared with traditional space (Khosrow-Pour 1998, p. 440; Robertson 2000, p. 248; Dodge and Kitchin 2001, p. 81). When a web page is surfed, what can be seen is only the display of information on the screen. The web site is not physically a reading room where people can read magazines, newspapers and books, listen to audio records or watch videos, nor a marketplace, bank, street, or forum. It is merely a collection of web pages written in various mark-up languages, comprised of letters, numbers, and symbols in common use, but which facilitate the functions of linkage to other media, communicating with other people or directing to other services. The electronic address is not necessarily located along a street, in a building or even in a city, province, or country. In addition, the online services are usually provided in the manner of a remote transaction paid by means of digital cash or virtual money. Finally, the Internet users include individuals and institutions, but they do not necessarily appear in person or in an entity in a

traditional library, forum, marketplace, bank, or along a street. It is entirely an invisible community in an invisible space—a group of anonymous netizens interact behind curtains or masks.

The invisibility of cyberspace worsens the situation caused by cyber anonymity, in the sense that criminals and offences in cyberspace become more concealed, while criminal justice faces greater difficulties.

Anonymity Symbolizes Cyberspace

The disappearance of physicality in activities on the Internet symbolizes the new way for daily routines, and presents a chance for new practice and changes in faiths, positions, and manners (Zigrus 2001, p. 171). To a certain extent, Internet services are provided for every user who owns a computer and a modem or cable linked to the server. The real identity of the user is not necessary for using the Internet. That is to say, a high degree of anonymity is achievable. Anonymity could indicate an intention to lie or not, to do something deceit or not. In the environment of online communications, particularly during interaction between remote strangers, information systems provide the possibility of maintaining anonymity, and we found that the users of information systems have the willingness to stay passively anonymous, not necessarily actively lying to their counterparts.

In the case of e-mail, it is uncomplicated to register an e-mail account with false information, or to send messages in the name of a certain person. These e-mails may not only infringe the legal rights and interests of the person of the counterfeited identity, but also are able to fabricate a rumour, slander other people, harm other people's reputation, or practise

unfair competition to reduce the competitor's trustworthiness. No obligation of free e-mail service providers has been established to investigate the registrants' identity information. In addition, some web sites also provide anonymous e-mail services or sell anonymous e-mail software (Examples of such services and software can be searched out with search engines). Under such circumstances, the traceback of the real sender is impossible. Only where the providers' status is clear, under vicarious liability, can it be useful for law enforcement in some jurisdictions to hold the re-publisher responsible for the content of the original author (Edwards and Walde, eds. 1997, Part 4).

E-mail has frequently been abused in an anonymous manner so as to realize a fraudulent scheme. This anonymity not only facilitates a lie, but may also support a fraud. In R. v. Mastronardi (2006 BCSC 1681), the accused, met the plaintiffs through an Internet dating service, during which the accused misrepresented himself as a single person and engaged in relationship with several victims. He represented himself as:

"(a) coming from a large, powerful and wealthy Sicilian family;

(b) being a widower seeking a wife;

(c) being a medical doctor with a specialty in gynaecology;

(d) having hospital privileges and a clinic;

(e) being a kind, caring and considerate person with positive family and moral beliefs, conveyed in conversations that went on for hours on end;

(f) having elaborate and sometimes bizarre family and cultural traditions requiring highly submissive wives and amalgamation of finances to an account controlled by him;

(g) as time went on, being third in command in mafia like family

organization;

(h) not wanting to date, but wanting to immediately enter into an intimate relationship, after which his culture and family regarded them as married;

(i) once so married, his family required him to follow family and cultural traditions.” (paragraph 4)

In R. v. Farkas, the accused engaged in online fraud by using different e-mail addresses, mailing addresses, and user names, victimizing sellers and purchasers distributed in the U. S., Canada, and England (2006 ONCJ 121, 10 April 2006). In R. v. Reynolds & Ors, the accused engaged in online chat claiming himself to be a 16-year-old boy, attempting to make young girls expose their bodies and transmit photographs to him over the Internet ([2007] EWCA Crim 538 (08 March 2007)).

There are many ways by which people make efforts to detect lies, usually including various clues to emotion that may disclose the situation of lying (Ekman 1992, as cited in Howitt 2002, pp. 251-253). However, in the electronic lie, none of the clues can be useful, particularly those emotional ones, because there is no face-to-face interaction. Rather, the interaction itself is covered by a human-machine-human fig leaf.

Another field where people usually maintain anonymity is interaction in chat rooms. Accounting for a considerable fraction of the income of the commercial online providers, chat systems support synchronous communication, discussion on different topics, trans-territorial relationships on common interests, and ignorance of social status (Internet Crime Forum IRC subgroup 2001, pp. 7-9; Rowland 1998; Wilbur 1997, p. 5.). The biggest advantage of the interaction in chat rooms is that the user can keep anonymous at the beginning of the chat or

remain anonymous during the whole process. Keeping anonymous means that people are able to fabricate identities that cannot be used to identify them. By disguising themselves, users can perpetrate fraud and many other related activities. This approach is definitely useful, too, in detection and investigation of crimes, where law enforcement uses falsified identity to allure and arrest suspects. For example, in United States v. Helder, (Eighth Circuit, No. 05-3387, 16 March 2006), an undercover officer used a screen name and claimed to be a 14-year-old girl to entrap the perpetrator (pp. 2-4); in United States v. Baker (Seventh Circuit, No. 05-2499, 24 January 2006), an undercover officer used a screen name and claimed to be a 14-year-old boy to entrap the perpetrator (pp. 2-3); in United States v. Antelope (Ninth Circuit No. 03-30557, 8 June, 2004. Docket num. 03-30334, January 2005), the accused joined an Internet site advertising "Preteen Nude Sex Pics" and started corresponding with an undercover law-enforcement agent, in respect of whom the accused was entrapped when he ordered a child pornography video over the Internet; in United States v. McGraw (Tenth Circuit No. 02-1407, D. C. No. 01-CR-426-B, 2 December 2003), the accused was also caught by an undercover agent, with whom he expressed his interests in "having sexual contact with 'white males between the ages of 12 and 15'," and arranged a encounter (See also R. v. Randall, Provincial Court of Nova Scotia 2006 NSPC 19, No. 1538177, 28 April 2006). The actual reality is that, in information systems, determining users' identity proves difficult, but not impossible.

Potentiality of Anonymity

Communicating anonymously is a great characteristic of the Internet environment. In using the Internet, anonymity can be kept from the beginning to the end. First, anonymous access to the Internet poses the most serious threat. In many countries, one of the most important forms of using the Internet is realized through cyber cafés or libraries, where anonymous users can access many of the online services. Definitely, there exist different situations in different countries. Compared with Finland where there are few cyber cafés in towns and cities, the cyber cafés in China have become the "third space" of school-aged juveniles besides home and school. The facilities and services in academic or public libraries are far less convenient for users than those in cyber cafés managed by private firms. An increasing number of hacking cases involving the Internet or Internet users are committed or conspired in cyber cafés.

Secondly, anonymous subscription to the Internet services raises the difficulty of identifying users. The personal information provided for the registration of an e-mail account, the name and address of e-mail messages, and the authors' information in Usenet, etc., can all be fabricated. Keeping identity anonymous is favourable for the protection of users from victimization, but it also favours the hiding of perpetrators from being traced.

Thirdly, users can keep their identity anonymous in the process of online communications. There are also mechanisms for keeping complete anonymity by which one user can send messages to other users, and then the messages are transmitted to the final target, such as newsgroup, e-mail list, or a single e-mail account. What makes it more complex is that in the mechanisms the intermediary can only be a programme and may be in another jurisdiction (Kingdon 1994). This also reminds us that there exists the possibility of numerous transmitting points, by which messages are transmitted from one terminal to the next terminal, from that to the

next in line, and so on, until the message reached the destination.

Tracing this transmitting process is theoretically possible. During the tracing process, the investigation is exactly the contrary to the process of transmission. Each time, the investigator can trace back one point.

It is likely that all points are identifiable. Nevertheless, as long as there is an unexpected element at any point, the tracing chain can be disrupted without reaching the original source. According to National Police Agency of Japan (1998), the possible examples include that the victim has no record of the Internet Protocol (IP) address; ISPs do not keep suitable records; hackers alter the logs; or some points are located in countries that have not criminalized hacking. As Koch (*Inter@ctive Week,* 10 July 2000) has pointed out, theories about detection remain theories, and they are too new to be tested in practice. Even if all the work of traceback is fulfilled, the actual value of this work may be discounted in a judicial process because of different locations and thus diversified jurisdictions.

Fourthly, the specific service or software can play further roles in hiding users. Cybercriminals usually establish anonymizers, which are systems particularly designed to invalidate technical identification of the source of communications (See Belgium's answer to the "Questionnaire 5: Have you received any reports from your law-enforcement authorities that have indicated an obstruction of their work due to the non-existence of appropriate legal instruments concerning traffic data retention?" in Council of the European Union, Council doc. 11490/1/02 CRIMORG 67 TELECOM 4 REV 1, Brussels, 20 November 2002). In fact, this kind of service or software can also be conveniently obtained free of charge or at an inexpensive price from the Internet. Everyone who is online can get access to these tools and services. Such software is likely to be replicated and spread unlimitedly, creating a bigger population of hidden users who

potentially threaten the security of information systems.

Although the anonymity of cybercriminals poses a series of questions, it is still the core of the "perfect environment" for the criminals. Levinson (2002, p. 455) said that anonymity is exploited by perpetrators of old crimes such as fraud, pornography, gambling, stalking and identity theft, or new crimes such as unauthorized access, denial of service, and malicious programmes. Yet it is at the same time welcomed by Internet users. People are constantly concerned that without online anonymity, it could be impossible to guarantee fundamental rights (COM(2000) 890 final, p. 20; National Police Agency of Japan 1998). It is not strange that the European Union Data Protection Working Party's Recommendation recognized that online anonymity brings about a dilemma for governments and international organizations (The Article 29 Data Protection Working Party 2001): in particular, in maintaining human rights to privacy and freedom of expression, and combating cybercrimes (COM(2000) 890 final, p. 20). Philip (2002) warned that anonymity can provide users with "the courage to do the outrageous and sometimes even resort to illegal activities."

Mitchell and Banker (1997, pp. 707-711) have concluded that there are four characteristics in which cybercrimes are different from traditional crimes, that is to say, difficulties in detection, limited reporting, jurisdictional complexities, and resource constraint. All these four aspects fall under the broad characteristic of concealment. The concealment of cybercrimes has been brought about by other technological and human factors (Conly 1991; Clark 1996; Stephenson 2000; Mandia and Prosises 2003; Mohay and co-workers 2003; Vacca 2005; Johnson 2006).

Most of traditional offences are greatly observable due to apparent depredations, presence of witnesses, and so on. There are also traditional

crimes that occur in private places and become less visible (Walsh 1983, p. 236). Unlike traditional threats where criminals are physically present at the crime scene, cybercriminals are usually not present at the crime scene thus making apprehension difficult (Speer 2000, p. 260). In information systems, executing a command to delete files does not mean that the files are permanently deleted. What happens is merely that files are hidden due to a change in file names so that the files can be recovered. In United States v. Angevine (Tenth Circuit No. 01-6097, D. C. No. 00-CR-106-M, 22 February 2002), "the computer expert used special technology to retrieve the data that had remained latent in the computer's memory," though the accused had attempted to delete the relevant files. In United States v. Upham (First Circuit No. 98-1121, 12 February 1999), the investigator used the "undelete" function of a programme to recover deleted files from the deposit media, as primary evidence in conviction. In Robertson v. Her Majesty's Advocate ([2004] ScotHC 11 (17 February 2004)), the police recovered 347 deleted images from the unallocated space, and 878 images and 45 movies from deleted zip file within the disc. Only when a secure-eraser programme is in use, the files are permanently deleted. For example, in the case of International Airport Centres, L. L. C., et al v. Jacob Citrin (Seventh Circuit No. 05-1522, 24 October 2005) (p. 2). Skilful criminals can disable this kind of security mechanism, and conceal the data that might possible be taken as evidence in prosecution.

Technological advances have both a positive impact on businesses and a negative impact on law enforcement (Institute for Security Technology Studies 2002). For example, in the DrinkOrDie case, the online software piracy group concealed its actions by various security measures: exchanging e-mails via private mail server using encryption; using a nickname to identify members, and communicating about group business only in closed, invite-only IRC channels; the FTP sites, where

tens of thousands of pirated software, game, movie, and music titles were deposited, were secured by particular authentication mechanisms (U. S. Department of Justice, Press release, 17 May 2002). On the other hand, the available technological solutions have not completely met the requirement of data collection, log analysis, and Internet protocol tracing (American Society for Industrial Security 2004, p. 40). There is also the necessity for law-enforcement agencies to recruit personnel with "electrical engineering and computer-science backgrounds" (Fields 2004, p. B1);

Inevitably, critics point out that cyber police have extra incentives than combating cybercrime, for example, asking for more money, more wiretap, bugs in computers and sell phones, weak encryption and permission to implement security technology, without more arrest following (Koch Inter@ctive Week, 10 July 2000).

Concealment of crimes has important economic effects. Stanley (1995, p. 2) stated that concealment of crime can decrease the incentives not to perpetrate, and increase the costs of law enforcement. Concealment of cybercrime demonstrates the low probability of punishment. In the U. S., only one in 100 cases was detected, one in 8 prosecuted, while only one in 33 prosecuted cybercrimes resulted in a prison sentence. That is to say, the likelihood that a cybercriminal would be put into prison was a one in 26,400 chance (Daler and co-workers 1989, p. 22), as compared with the likelihood of imprisonment in traditional bank robbery a one in three chance (ibid.). Law-enforcement agencies found that a majority of cybercrimes never reached the criminal-justice system. Even in the relatively few cases where a crime was reported, most often the criminal's identity was never discovered. As a consequence, as Radzinowicz and King (1977, p. 67) pointed out, "The calculation of chance is as applicable to the commission of crime as to many other activities." Given other

factors constant, if cybercrime is more concealed than other offences, the potential perpetrators are more motivated to take illegal actions on the Internet, and thus more offenders of traditional crime will be prepared to migrate to cyberspace.

Trans-territorial Anonymity

Free flow of information from one state to another is a purpose of information systems (Directive 95/46/EC, Preamble (3); UN A/RES/51/162; Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 12), but trans-border flow is not free (The Convention mentioned above, Article 12 provides the limit on trans-border transfer of data). The trans-border information flux is accompanied by risks of crime of a similar nature. In any country, the court must have jurisdiction over the person or the subject-matter of a lawsuit. This works well with the current set-up of law-enforcement agencies that are territorial and are operating in different villages, towns, districts, cities, counties, states or provinces, or national boundaries. Nevertheless, unauthorized access to information systems can be accomplished from virtually anywhere on the networks (See cases such as United States v. Tenebaum (Israel), 18 March, 1998, involving an Israeli hacking United States military computers; United States v. Gorshkov (W.D. Wash) 4 October 2002, Russian hacker; United States v. McKinnon I (E.D. Va.) and II (D. N.J.) 12 November 2002, British National Hacked into the U. S. Military Networks; United States v. Zezev (S.D. N.Y.) 1 July 2003, Hackers from Kazakhstan; United States v. Ivanov (D. Conn.) 25 July 2003, Russian hacker), because the

communications capability of cyberspace allows criminals to conspire more easily, without geographical proximity to one another or to the target (Lenk 1997, pp. 126-135). The international characteristic of cybercrime is evident (National Police Agency 1998). In fact, some of the cases prosecuted have been of this nature, for instance, R. v. Kozun (2007 MBPC 7), where the forensic analysis of the computer of the accused disclosed that 165 separate users from 15 countries had traded through his computer. The computer was converted into an automated trading centre through a programme, by which 141 users had traded in the previous 13 days.

The sphere of legal jurisdiction makes the cybercrime enforcement more complicated (Lee and co-workers 1999, p. 873). Smith, Grabosky, and Urbas (2004) concluded that the trans-national dimension of cybercrime posed four formidable challenges for prosecutors, who have to determine whether the conduct in question is criminal in their own jurisdiction, collect sufficient evidence to mobilize the law, identify the perpetrator, and determine his or her location, and decide whether to leave the matter to the local authorities or to extradite the offender (pp. 48-49).

Sinrod and Reilly (2000, p. 2) have pointed out that although some international organizations are examining cooperative mechanisms in the field of fighting against cybercrime, many of their members are slow in recognizing the urgency of the situation.

The elimination of borders favours inter-jurisdictional mobility of crime. Due to the actual difficulty in establishing jurisdiction, even if a certain offence is detected, it is still uncertain whether the way can easily lead to punishment. In R. v. Burns ([2003] NICC 13(2) (12 September 2003)), where the accused cloned mobile phones, or exploited faults or loopholes in the internal phone systems of companies or organizations to

make cheap or free calls at the expense of those companies or organizations, the court found that:

"As the investigation progressed it became more wide-ranging and involved another suspect and its ramifications were such that it eventually spread to other parts of the United Kingdom, to Tokyo, to South America, as well as to New Jersey and Atlanta in the United States of America. Several large organizations in the United Kingdom, other police forces and international telephone companies were involved. When it became apparent to the police that they did not have either the specialist equipment or the necessary expertise to access much of the information, specialist firms had to be engaged. All of this took a great deal of time." Reasonably, suggestions have been made to incorporate cyberspace into various jurisdictional frameworks. Nonetheless, this needs a great deal of time, agreement, and co-operation between countries, which are still struggling to take common actions.

Finally, it is worth noting that trans-national cases just make up a inconsequential part of cybercrime. No convinced conclusion can be drawn because it is probable that trans-national offences are not as prevalent as scholars have assumed. On the other hand, it is difficult to reveal these offences for reasons that scholars have laid bare. Or, it may be, that it is simply law enforcement does not put sufficient emphasis on these offences. Before credible data are available to give an answer to this question, we have certain reasons to claim that trans-national offences have sometimes of a dual nature: they do not appear as prevalent as domestic offences, but they are more difficult to detect and convict. In addition, because the investigation of trans-national offences is more expensive and time-consuming, law enforcement will not give more priorities to these offences than to cases that have happened "close to home".

Because information systems alone are no longer subject to the

physical limit of traditional countries, we can expect that many offences traditionally committed in neighborhoods, communities, and native areas now extend beyond national boundaries. Many other offences traditionally committed in a trans-border manner are becoming a means to acquire new markets in the more networked globe. Some new offences can, indeed, only be completed in a trans-national style. Trans-national crime can be seen as the counterpart of international trade in civil society, being an involuntary transaction between perpetrators and the social order (in many cases, involving victims, but in many other cases, victimless).

For example, in McKinnon v USA & Anor ([2007] EWHC 762 (Admin) (03 April 2007)), the accused used his own computer in London and obtained unauthorized access to dozens of governmental computers of the U. S., from which he discovered the identities of certain administrative accounts and associated passwords. He installed remote control software on these administrative computers. The software enabled him to access and change data at any time.

Many people have taken it for granted that because computer networks are trans-national, naturally most crimes committed in relation to the networks are also trans-national. This poses a great concern among academia, law-enforcement agency, and legislature. However, this is still an unanswered question: firstly, information systems have crossed the national boundaries, but prosecuted offences are mostly confined within these boundaries; secondly, due to lack of an international arrangement of law and enforcement, few trans-national cybercrime offenders have been investigated; and thirdly, offences are mostly territory-dependent, and do not cross the border at all.

All these factors are responsible for the low likelihood of trans-national cybercrime, but, as we have seen and will see further, the absence of international legal harmonization and assistance mechanisms

contributes primarily to the current invisibility of trans-national cybercrime.

Impact of Cyber Anonymity on Criminal Motivation and Victimization

Lack of punishment reduced the expected cost of the criminals, which were composed thus of moral costs and substantial costs, specifically, the perpetrators' necessary devices and labour in cybercrime. Because there was no cybercrime law, there was neither expected punishment nor the expected cost induced by the expected punishment. Under such circumstances, the probability of conviction equalled zero. The expected utility of the perpetrator almost equalled the utility of a situation in which crime went undetected or unpunished. According to an economic analysis of crime (Becker 1968, pp. 169-217), those who are risk-indifferent are indifferent to detection and conviction. For those who are risk-lovers, cybercrime becomes a new cause, a new chance, a new challenge, and a new type of risk. For those who are risk avoiders, because of the low risk of detection and conviction rate of cybercrime, they transfer from other offences to cybercrime. Therefore, the number of cybercrimes and perpetrators will inevitably increase.

The low cost of cybercrime and the difficulty in detection and evidence collection create incentives for potential perpetrators. The nature of high intelligence, trans-territoriality, and high concealment of cyber transgress and cybercrime make it difficult to detect and investigate the cases (See Conly 1991; Clark 1996; Stephenson 2000; Mandia and Prosises 2003; Mohay and co-workers 2003; Vacca 2005; Johnson 2006). Stating from

another standpoint, cybercrime surpasses the current capacity of public and private regulators to control (Grabosky 2000, p. 2). As for the transgressors or criminals, they usually only need to click the mouse or knock the keyboard at home or in the office in order to commit the illegality in a short time. The risks and costs are in cybercrime lower than those in traditional crime, while the benefits are higher. This cost-effectiveness further strengthens the mind of the perpetrator to commit cybercrime.

Cybercriminals have a greater advantage than most of the traditional criminals in respect of the low probability of arrest and conviction. Hatcher and co-workers (1997, pp. 397, 399.) have pointed out that many cybercrimes are not reported. The term “dark figure”, used by criminologists to refer to unreported or unrecorded crime, has been applied to denote undiscovered cybercrimes (UNCJIN 1999, Paragraph 30). As Radzinowicz and King (1977) pointed out that, “The recorded figures of crime are huge but the reality behind them everywhere looms far larger. The sinister word dunkelziffer (dark figure) was coined at the turn of the century to express this hidden reality.” (p. 42). Many intrusions are not detected for a variety of reasons (COM (2000) 890 final, p. 11). Cybercrimes can well be described as hidden crimes, which is used by Cook (1997) to denote under-reported or under-recorded crimes such as domestic violence, sexual assault, and racial harassment (p. 55-58), the counterpart of which is “hidden victims,” denoting the victims of the “hidden crimes” (p. 127).

At the same time, victims of cybercrime are keen to be hidden victims (Cook 1997, p. 127). The usual “motives for silence” pertaining to victimization may fall into one of the following categories: 1. The idea that the victimization is not worth the mobilization of justice; 2. Involvement; 3. Pressures of fear; 4. The perturbed accessibility of police and court; and

5. The ignorance of events by the police (Radzinowicz and King 1977, pp. 38-40).

In sketching the victim decision-making, Greenberg and Ruback (1985) have established a three-stage model: the victim judges whether the event is a crime, evaluates its seriousness and decides what to do (Greenberg and Ruback 1985, as cited by Feldman 1993, p. 26). Before these stages, one stage that is more essential should be included, that is, whether the victim knows the event. If this is the case, the reporting of cybercrime might stay at a lower level, because cybercrime is imperceptible and thorny to notice; it is much trickier for the victim to judge whether the event is a crime and to estimate the losses; and the victim has less awareness of whether there is an agency to report the crime. The limited reporting of the cybercrime has been noted more than 20 years ago by Parker and Nycum (1984, p. 313), who studied the invisibility of computer crime. At present, the Internet's virtual environment has made the circumstances still poorer. Auspicious progress in proving material evidences in traditional crimes was made in late 1980s when DNA tests were first introduced (Levinson 2002, p. 537). Nonetheless, digital evidence in computer crime is untouched by such high-technological testing measures. The invisibility of cybercrimes is based on numerous factors, either technical or artificial (UNCJIN 1999, Paragraphs 30, 31). Sometimes, the straightforward cause is that the victims are not enthusiastic to report, or even do not know where to report the case (Salgado 2001). The acknowledged reasons for the reluctance to launch legal actions are principally fear of undesirable publicity, public humiliation or loss of goodwill, loss of investor or public confidence, resulting economic consequences such as the panic effect that this information would create on their stock prices (See Carter 1995, p. 21; Roush 1995, pp. 32, 34; Gelbstein and Kamal 2002, p. 2; McKenna 2003),

and exposure to future attacks (COM (2000) 890 final, p. 11). The UN suggested that these factors have a momentous impact on the detection of cybercrime (UNCJIN 1999, Paragraph 31).

Yet there are other reasons for the victim to remain silence. While many people are vigorous in maintaining their interests and rights, some people view victimization as their own malfunction in life and profession and are not enthusiastic to expose the reality of their failure to any individuals and institutions, so as not to make public their own disadvantage.

Therefore, it is unavoidable that the rate of unidentified instances of cybercrimes has increased as a consequence. The 2013 Australian Cyber Crime and Security Survey Report summarized the reasons why respondents did not report cyber security incidents, 44% of them said "there are no benefits of reporting"; 44% chose "other", meaning that the incidents and the consequences were minor, and that the incidents were reported internally and managed by corporate policy; 20% said that "the attackers probably wouldn't get caught &/or prosecuted"; 16% of them "did not know"; and 12% worried about "negative publicity for the organisation" (CERT Australia 2014, p. 35). This and other similar surveys has indicated the percentages of respondents identifying each stated rationale as being very imperative in their assessment not to report computer intrusion. At the same time, it is worth noting that the reasons are subject to changes in each yearly study.

Conclusion

Without ignoring all its merits, cyber anonymity has deep impact on

occurrence of cybercrime, mostly reducing the potential likelihood of detection and thus its costs. In fact, anonymity may to some extent encourage potential perpetrators to take the risk. On the other hand, victims may lose opportunities to make judgment on whether or not it is of their interest to interact with hidden perpetrators. Once crime occurs, anonymity further hinders law enforcement from detecting and investigating.

In recent year, wrestling between claims for and against cyber anonymity has been continuing. However, there has some new advancement in judicial sector. The European Union Court of Justice issued a decision on May 13 2014, in case C-131/12 (Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez), ruling that the "right to be forgotten" is embedded in the provisions of Directive 95/46/EEC (Iglezakis 2014, p. 4). The right to be forgotten is a special field of cyber anonymity. If cyber anonymity is not imposed any limit, vulnerable users and incompetent law enforcement cannot cope with problems accompanying it. Therefore, the right to be forgotten applies only where the information is "inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing" (para 93 of the ruling). the Court unambiguously spelt out that the right to be forgotten is not unconditional but will always have to be "balanced against other fundamental rights", for instance the freedom of expression and of the media (para 85 of the ruling). Absolute freedom of anonymity should not be allowed as the case in the real society. There is a necessity to balance the needs to protect privacy and prevent cybercrime (Shinder, 2011).

References

1. American Society for Industrial Security (ASIS). 2004. Cybercrime-Fighting Tools Still Lacking, *Security Management*, no. 40.
2. Becker, G. S. 1968. Crime and Punishment: An Economic Approach, *Journal of Political Economy*, vol. 76, pp. 169-217.
3. Carter, D. L. 1995. Computer Crime Categories, *Law Enforcement Bulletin*, U. S. Department of Justice: Federal Bureau of Investigation, vol. 64, no. 7, pp. 21-26.
4. CERT Australia. 2014. The 2013 Australia Cyber Crime and Security Survey Report. Commonwealth of Australia.
5. Clark, F. and Diliberto, K. 1996. *Investigating Computer Crime*, Boca Raton, Florida: CRC Press LLC, 1996.
6. Commission of the European Communities. 2000. *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime,* COM (2000) 890 final.
7. Conly, C. H. 1991. *Organizing for Computer Crime Investigation and Prosecution*, Darby, PA: Diane Publishing.
8. Cook, Dee. 1997. *Poverty, Crime and Punishment*, London: CPAG.
9. Daler, T., Gulbrandsen, R., Melgrd, B. and Sjølstad, T. 1989. *Security of Information and Data*, Chichester: Ellis Horwood.
10. Debose, B. 2004. Kerry Says Threat of Terrorism Is Exaggerated, *The Washington Times,* 29 January.
11. Dodge, M. and Kitchin, R. 2001. *Mapping Cyberspace*, New York, New York: Routledge.

12. Edwards, L. and Walde, C. (eds.). 1997. *Law and the Internet - Regulating Cyberspace*, Oxford: Hart Publishing.

13. Ekman, P. 1992. *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*, New York: Norton.

14. European Commission. 2014. Factsheet on the right to be forgotten ruling C - 131/12. Retrieved 5 Feb. 2015, from http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

15. Fields, G. 2004. Cyberexperts and Engineers Wanted by FBI, *Wall Street Journal*, B1, 6 April.

16. Gelbstein, E., and Kamal, A. 2002. *Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security*, the United Nations Information and Communications Technology Task Force and the United Nations Institute for Training and Research.

17. Grabosky, P. 2000. Cyber Crime and Information Warfare, in Proceedings of the Transnational Crime Conference, Canberra, 9-10 March. Retrieved 5 Feb. 2015, from http://www.aic.gov.au/conferences/transnational/grabosky.pdf

18. Greenberg, M. S. and Ruback, R. B. 1985. A Model of Crime Victim Decision Making, *Victimology: An International Journal*, vol. 10, pp. 600-616.

19. Hatcher, M. and co-workers. 1999. Computer Crimes, *American Criminal Law Review*, vol. 36.

20. Howitt, D. 2002. *Forensic and Criminal Psychology*, Essex, England: Pearson.

21. Hunt, Allan. 1993. *Explorations in Law and Society: Towards a*

Constitutive Theory of Law. New York, London: Routledge.

22. Iglezakis, I. 2014. The Right to Be Forgotten in the Google Spain Case (Case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet? Retrieved 5 Feb. 2015, from http://dx.doi.org/10.2139/ssrn.2472323

23. Institute for Security Technology Studies (ISTS). 2002. *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment*.

24. Internet Crime Forum IRC Subgroup. 2001. *Chat Wise, Street Wise-Children and Internet Chat Services*.

25. Internet World Stats. 2014. World Internet Usage and Population Statistics – June 30, 2014 Mid-Year Update. Retrieved 5 Feb. 2015, from http://www.internetworldstats.com/stats.htm

26. Johnson, T. A. 2006. *Forensic Computer Crime Investigation*, Boca Raton, Florida: Taylor and Francis Group.

27. Khosrow-Pour, M. 1998. *Effective Utilization and Management of Emerging Information Technologies*, Hershey: Idea Group Publishing.

28. Kingdon, J. 1994. Shooting the Messenger: The Liability of Internet Service Providers for Prohibited Expression. Retrieved 5 Feb. 2015, from http://www.catalaw.com/logic/docs/jk-isps.htm

29. Koch, L. Z. 2000. Open Sources Preventing Cybercrime, *Inter@ctive Week*.

30. Lee, M. and co-workers. 1999. Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal, *Berkeley Technological Law Journal*, vol. 14, no. 2, pp. 839-885.

31. Lenk, K. 1997. *The Challenge of Cyberspatial Forms of Human*

Interaction to Territorial Governance and Policing, The Governance of Cyberspace, New York: Routledge, pp. 126-135.

32. Levinson, D. (ed.). 2002. *Encyclopaedia of Crime and Punishment*, Newbury Park, CA: Sage Publications.

33. Li, X. 2008. *Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society*, Turku: Uniprint.

34. Mandia, K. and Prosise, C. 2003. *Incident Response and Computer Forensics*, Emeryville, California: McGraw-Hill/Osborne.

35. McKenna, B. 2003. United Kingdom Police Promise Charter to Guard Good Names, *Computers and Security*, vol. 22, no. 1, pp. 38-40.

36. Mitchell, S. D., and Banker, E. A. 1998. Private Intrusion Response, *Harvard Journal of Law and Technology*, vol. 11, no. 3, pp. 699-732.

37. Mohay, G., Byron, C., Vel, O., McKemmish R., and Anderson, A. 2003. *Computer and Intrusion Forensics*, Norwood, Massachusetts: Artech House.

38. NPA. 1998. *The Situation of High-tech Crime and the Suppression of Police, Japan Police White Paper*, Tokyo: National Police Agency.

39. O'Brien, T. 2004. Risk and Conflict Challenges for New Zealand, *Auckland War Memorial Museum Symposium Push for Peace*.

40. OECD. 2004. *Second Organization for Economic Cooperation and Development Workshop on Spam: Report of the Workshop*, JT00174847, Busan, Korea.

41. OECD. 2005. Task Force on Spam, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, Paris, France.

42. Parker, D. B., and Nycum, S. H. 1984. Computer Crime, *Communication of the ACM*, vol. 27, no. 4, pp. 313-315.

43. Philip, A. R. *The Legal System and Ethics in Information Security*, SANS Institute, 2002. Retrieved 5 Feb. 2015, from http://www.securitydocs.com/go/1604

44. Radzinowicz, L. and King, J. 1977. *The Growth of Crime: The International Experience,* London: Hamish Hamilton.

45. Robertson, S. 2000. The Digital City's Public Library: Support for Community Building and Knowledge Sharing, in Toru Ishida and Katherine Isbister (eds.) *Digital Cities: technologies, Experiences, and Future Perspectives*, Springer, pp. 246-260.

46. Roush, W. 1995. Hackers: Taking a Bite Out of Computer Crime, *Technology Review*.

47. Rowland, D. 1998. Cyberspace - A Contemporary Utopia? *The Journal of Information, Law and Technology*, vol. 1998, no. 3. Retrieved 5 Feb. 2015, from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_3/rowland/

48. Salgado, R. P. 2001. Working with Victims of Computer Network Hacks, *USA Bulletin*, vol. 49, no. 2.

49. Shinder, D, 2011. Online Anonymity: Balancing the Needs to Protect Privacy and Prevent Cybercrime. Retrieved 5 Feb. 2015, from http://www.techrepublic.com/blog/it-security/online-anonymity-balancing-the-needs-to-protect-privacy-and-prevent-cybercrime/

50. Sinrod, E. J., and Reilly, W. P. 2000. Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, *Computer and High Technology Law Journal*, vol. 16, pp. 177-232.

51. Smith, R. G., Grabosky, P. and Urbas, G. 2004. *Cyber Criminals on Trial*, Cambridge: The Press Syndicate of the University of Cambridge.

52. Speer, D. L. 2000. Redefining Borders: The Challenges of Cybercrime, *Crime, Law and Social Change*, vol. 34, pp. 259-273.

53. Stanley, T. J. 1995. Optimal Penalties for Concealment of Crime, *Economics Working Paper Archive*.

54. Stephenson, P. 2000. *Investigating Computer-Related Crime*, Boca Raton: Florida: CRC Press LLC.

55. The Article 29 Data Protection Working Party. 2001. Fourth Annual Report on the Situation Regarding the Protection of Individuals with Regard to the Processing of Personal Data and Privacy in the Community and in the Third Countries Covering the Year 1999.

56. UNCJIN. 1999. International Review of Criminal Policy -United Nations Manual on the Prevention and Control of Computer-Related Crime, *International Review of Criminal Policy*, nos. 43 and 44.

57. Vacca, J. R. 2005. *Computer Forensic: Computer Crime Scene Investigation*, Hingham, Massachusetts: Charles River Media.

58. Walsh, D. P. 1983. Visibility, in Dermot Walsh and Adrian Poole (eds), *A Dictionary of Criminology*, London, Boston, Melbourne and Henley: Routledge and Kegan Paul.

59. Weimann, G. 2004. Cyberterrorism: How Real is the Threat? *United States Institute of Peace Special Report*, no. 119.

60. Wilbur. S. 1997. An Archaeology of Cyberspace: Virtuality, Community, Identity, in D. Porter, (ed.), *Internet Culture*, London: Routledge, pp. 5-22.

61. Yi, M. 2006. Associated with Traditional Crime, Cybercrime Threats Citizens Safety, *Huanghai Morning Newspaper*, 27 January.

62. Zigrus, I. 2001. Our Virtual World: The Transformation of Work, Play, and Life via Technology, IGI Global.

CHAPTER IV HALLMARKS OF PROSECUTED CYBERCRIME

Introduction

The social change of recent decades has been primarily symbolized by the development of information and communications technology. One of the most significant negative impacts in this context is the emergence and rampancy of cybercrime. The research on criminal phenomenon related to information and communications technology has become a focus of criminology, criminal law and information security.

Cybercrime is a comprehensive topic and attracts scholars from different disciplines to deal with. Many have been written about the theoretical explanation of cybercrime. Many findings about cybercrime in different studies revealed different dimension of multi-dimensional phenomenon. While the limited previous first-hand exploration have been widely accepted and cited, controversies and misleading exist among various studies. The unfortunate situation is that, in the field of profile of cybercriminal and cybervictim, most subsequent theoretical treatises tend to provide proofs for the earliest findings, or at most provide some tiny

revisions.

It is critical to answer the questions of “who are most possible to commit cybercrime? And, who are most possible to be victimized in cybercrime?” or “how the cybercrime perpetrators and cybervictims look like?” The subjects of cybercrimes lead the tide of the theory and practice of legislation and law enforcement in the sense that the perpetrators are those who challenge the traditional legal system. The studies and research on subject of computer crime has had a history of several decades, and established well-known profile for the cybercriminals and cybervictims.

With the deepening of the research on cybercrime, the hallmarks of cybercriminals and the guardianship of cybervictims are paid increasing attention by lawyers and law enforcement. The purpose of this study is to present an updated profile of cybercriminality and cybervictimization, through the analysis of 115 typical cybercrime cases prosecuted in the United States of America during 18 March 1998 to 12 May 2006 and published on the Department of Justice web site.

Literature review

When we talk about subjects of cybercrime, we are concerning the profile of cybercriminal. However, cybercriminal is not one single person, but represents a school of perpetrators. Many have been written in the previous literature about “who” would be the one who are most likely to commit cybercrime and “who” would be likely to be victimised in cybercrime. Any conclusions drawn from some hundreds or thousands of cases might be premature or even misleading. More than 20 years ago,

Bequai (1983, p. xviii) pointed out that, the problem of computer criminal profile could be much complex and no one single picture could be given to sketch the panorama of this aggregation. Bequai (1983, pp. 42-45) gave a tentative table of profile of typical computer perpetrator, assembled from hundreds of cases involved in the United States Bureau of Justice statistics. He had the same worry about the misleading effect as many other scholars did.

Bequai (1978, p. 4) presented that:

"Studies of computer criminals usually portray them as young, educated, technically competent, and usually aggressive. Some steal for personal gain, others for the challenge, and still others because they are pawns in a larger scheme…Still other studies typically portray computer criminals as technicians, managers, and programmers. They are usually perceived as jovially challenging the machine, and discovery occurs only through inadvertence. The theft usually involves money, services, or trade secrets. However, when caught, the computer criminal's sentence is light compared to that of traditional property-crime felons, who usually receive harsh sentences for crimes involving much less property or money."

It has been widely recognised that there is no single profile that can capture the characteristics of a "typical" computer criminal, and many who fit the profile are not necessarily criminals at all (Ware, Pfleeger and Pfleeger 2002, p. 20). Donn B. Parker (1976) has presented a brilliant portrait of a computer crime perpetrator:

"Perpetrators are usually bright, eager, highly motivated, courageous, adventuresome, and qualified people willing to accept a technical challenge. They have exactly the characteristics that make them highly desirable employees in data processing."

The development of the computer technology has changed the depiction completely (Becker 1981). Becker (1981) suggested seven views of computer system: the playpen, the land of opportunity, the cookie jar, the war zone, the soapbox, the fairyland, and the toolbox (pp. 18-20). Bequai (1983, pp. 47-50) researched the potential sources of computer attack might vary from each other, but could be grouped into three categories: dishonest insiders, outsiders, and users. It implied that everyone has an equal chance to be involved in computer crime, in the age when the Internet did not expand as wide as present. Wasik (1991, pp. 60-65) concentrated on the characteristics and classifications of perpetrators as well. Levinson (2002) sorted courses of cyber threats into five groups, including insiders, hackers, virus writers, criminals groups, and terrorists (Levinson 2002, p. 525). Reynolds (2003, pp. 58-65) classified perpetrators into hacker, cracker, insider, industrial spy, cybercriminal and cyberterrorist. That is to say, the spacious application of computers created a multi-dimensional social environment, and the potential computer criminals inevitably discovered the opportunities.

The Internet users worldwide are strongly sex divided, that is, a higher percentage of males than females use Internet. For example, in 2001, only 6 per cent of Internet users in the Arab States are women; 38 per cent in Latin America; 25 per cent in the EU; 37 per cent in China, 19 per cent in Russia, 18 per cent in Japan, 17 per cent in South Africa, and nearly 50 per cent in the United States are women.[1] However, the distance is increasingly smaller; with females constitute the lager group of Internet users in some countries. In Nordic countries, it was found that also male have a higher percentage of daily users of the Internet (Nordic Council of Ministers 2005, p. 42, Table 2.5).

[1] Women's Learning Partnership, December 2001, http://learningpartnership.org/facts/tech.phtml

The previous studies proved that cybercrime is far more sex divided than the Internet use. According to Levinson (2002), "It is well established that boys commit far more juvenile crime, particularly violent crime, than girls." (p. 490) The cybercrime seems less violent, but the research indicated that more males commit cybercrimes than female. According to Jiang (2000), males constitute 91.45 percent of the perpetrators in a statistics, while females constitute only 8.55 percent. He supposed the differences of computer knowledge and skills and the attitudes in online interactions between males and females resulted in this situation (pp. 151-152). However, the reasons why the females have found less guilty of cybercrime than males are not clear at all. It needs specific search to answer the questions such as: "Do females commit less cybercrimes?" "Are female cybercriminals less detected?" or more philosophically, "Can we measure criminal phenomenon among males and females under the same concept?" But this study is not intended to answer these questions.

A noteworthy phenomenon is that, in regardless of individual cybercrimes, corporate cybercrime, or organized cybercrime, the young perpetrators play a critical part. Although there is no age limit to commit cybercrime, we found that similar to traditional crimes, the youth constitute an important part of the cybercriminals. As Shannon (1993, p. 2) reported that, cybercriminals tend to usually be between the ages of 14-30, they are usually bright, eager, highly motivated, adventuresome, and willing to accept technical challenges. The age of criminal responsibility is prescribed different between countries. In most countries, children less than 14 or 15 years of age are not liable for the criminal offence, while children between 15-17 or 14-16 years of age are liable for limited range of offences.[2] In fact, juveniles commit a number of these crimes. In China,

[2] For example, in China Penal law, children under 14 years old of age are not liable; in Finland Penal law, the age limit is 15. In some other countries, the liability age is even lower. In England and Wales, the age is 10-year-old, while the limited liability ages are between 10-14 years of age.

the Internet users between the ages of 19-40 make up 80 percent of all users, and the average age of the cybercrime perpetrators is 23 years old (Dong 2003). Juvenile delinquency and juvenile justice became issues closely associated with cybercrime. According to findings of criminal psychological research, the reason why the children are more likely to commit crime is not because more and more children will commit crime, but because most of the potential offenders will commence to commit crime in childhood and continue their criminality for much of their lifetime. After 16-17 years of age, the offending rates decreases to a plateau (Howitt 2002, pp. 76-77).

Underwood (2002) found that the cybercriminal behaviour cuts across a broad range of society, with the age of most offenders ranging from 10 to 60 years. People between the ages of 20 and 59 make up 94 percent of computer criminals, with the most active being people in their thirties.

Bequai (1983, p. 43, Table 1)'s profile of typical computer felon presented a full portrait of the above mentioned aspects, with more other aspects. He stated that the age of computer criminals is between 15-45 years old. Males are responsible for most computer crimes, but females are increasing. The occupational experience of computer criminals differs from the highly experienced technician to a minimally experienced professional. Both public and private sectors could be the victims of the computer crimes. The computer criminals have the personal traits of being bright, motivated, and ready to accept the technical challenge; usually a desirable employee, a hard and committed worker. Computer crimes are mostly by individual perpetrators, but conspiracies are increasing. Most offences are committed by insiders who have easy access to the computer system. The security of the victims' system is usually slack.

It has been an important topic to distinguish the sources that the

offenders come from and the relationship between the offenders and the victims, by which computer crimes can be divided into offences by insiders and offences by outsiders. Shaw, Ruby and Post (1998) classified insiders into information technology specialists such as full-time or part-time employees, contractors, consultants, or temporary workers; partners and customers with system access; and former employees retaining system access. About whether the insiders or the outsiders constitute the greatest threat to the computer system, there have been different findings.[3]

However, the mainstream findings support the view that the insiders have been more likely to be involved in computer crimes against the employers' systems. The Nordic Council of Ministers (2005) found that students, employees and self-employed people constitute the higher percentage of the Internet penetration (Nordic Council of Ministers 2005, p. 42, Table 2.5). Mackenizie and Goldman (2000) reported that some students, particularly computer science and engineering majors, with newly discovered skills attempt to break into the servers of University of Delaware (p. 174). Meta Group (2004) found that, of more than 1,600 information and communications technology professionals, current employees represent the biggest threat to technology infrastructures. Computer Security Institute and Federal Bureau of Investigation reported that 55 percent of survey respondents reported malicious activity by insiders (Nelson 2004). Researchers also revealed that the dissatisfied employees are a major source of computer crimes (Vatis 1999) and are the greatest threat to a computer's security (Sinrod and Reilly 2000, pp. 183-187). When Sutherland suggested the term "white-collar crime" in the late 1930s, he might hardly imagine that there would be crimes in the process

[3] For example, The AFCOM's Data Centre Institute found that the cyber attacks launched by outsiders (52 percent) were ten times that of the insiders (5 percent). However, the respondents were more concerned the insider threats than the outsider ones. See Edward Hurley, Are Insiders Really a Bigger Threat? 17 July 2003. Retrieved 26 June 2006, from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci906437,00.html

of human-machine interaction, other than the human-human interaction, human-organisation interaction, or human action against machine. Nevertheless, the term "white-collar cybercrime" also came into being at present as a contribution to develop Sutherland's theory.[4]

Besides the revealed relationship between the criminals and victims, others also explored the characteristics of victims. Syngress (2002) summarized the common victim characteristics include those who are new to the Internet; who are naturally naïve; who are disable or disadvantaged; who are greedy, lonely, or have other emotional needs; pseudo-victims who report having been victimized but actually were not; and who are simply unlucky enough to be in the wrong (virtual) place at the wrong time.

From the previous literatures, the profile of cybercriminal and cybervictim could hardly be regarded as settled. In addition, the available literatures did not provide detailed sources of materials and clarify their methods. Many literatures have apparently been based on second-hand materials and/or mass media reports. There is still a need of findings about the hallmarks of cybercriminals and cybervictims drawn from the prosecuted cases.

Methods

The study used a sample of 115 reported typical cases sentenced or on trial (during 18 March 1998 to 12 May 2006), published on the web site of

[4] See for example, "Victim Assistance Online" Web site. Retrieved 8 July 2006, from http://www.vaonline.org/internet_wcollar.html. The term "White-Collar Hacker" is also used, for example, by Leyden, J. The Rise of White Collar Hacker, 2004. Retrieved 8 July 2006, from http://www.theregister.co.uk/2004/03/31/the_rise_of_the_white/

the United States Department of Justice. The study took all the cases listed in the web page located at <http://www.cybercrime.gov/cccases.html>. About the nature of these cases, the web page gives a note as:

"Below is a summary chart of recently prosecuted computer cases. Many cases have been prosecuted under the computer crime statute, 18 U.S.C. §1030. This listing is a representative sample; it is not exhaustive."

The study classified the sample cases into hacking and illegal access; attack, sabotage and botnet; viruses, worms, spyware and logic bomb; data theft and espionage; ID theft, fraud; and miscellaneous including embezzlement and corruption. The strict legal categorization is not used in this study. Rather, the classification is based on criminological characteristics of the behaviours.

The statistical items include those related to the demographic characteristics of the cybercriminal (including gender, age, insider or outsider, American citizen or foreigner), the nature of the victims (including private, public, private and public, and public health and safety), the losses of the cases, and the decided punishments on the cybercirme (imprisonment and fine), the guardianship level of the victim (classified into strong, medium, and weak), and the complexities of techniques involved (classified into complicated, medium, and simple).

Results

1. Gender distribution of cybercrime

In most categories of offences, male offenders constitute the absolute majority of the criminals. Only two female offenders are reported in hacking and illegal access, one reported in miscellaneous offences (including embezzlement, corruption, and so on). The overall male offenders constitute more than 98 percent of the total perpetrators, while the female are only less than two percent.

2. Age distribution of cybercrime

The report from the website is incomplete in providing offenders' age information. The non-available age information exists in every category of offence. About 73 .1 percent of offenders of ID theft, 30.4 percent of attack, sabotage and botnet, 18.2 percent of viruses, worms, spyware and logic bomb, 15.9 percent of hacking and illegal access, 14.3 percent of both data theft and espionage, and miscellaneous (including embezzlement and corruption) are absent.

Three perpetrators with the age of younger than 16 years old are convicted with offences in the categories of hacking and illegal access, and viruses, worms, spyware and logic bomb.

The offenders of the age older than 46 years old distribute in most categories of offences, except fraud and miscellaneous (embezzlement and corruption). However, generally they are not active in computer crime and constitute a small percentage of the total reported offenders (including the offenders whose ages are non-available): about 28.6 percent of offenders in data theft and espionage, mote than 9 percent of viruses, worms, spyware and logic bomb, four percent of attack and sabotage, and 3.8 percent of ID theft.

The cyber criminals distribute obviously among the ages between 17

to 45 years old. Offenders among those approximately 79.3 percent of hacking and illegal access, approximately 65.2 percent of attack and sabotage, approximately 63.7 percent of viruses, worms, spyware and logic bomb, approximately 85.8 percent of data theft and espionage, approximately 26.8 percent of ID theft, exactly 100 percent of fraud, and approximately 85.7 percent of miscellaneous (embezzlement and corruption), are between the age of 17 to 45 years old.

More detailed distribution of offenders with the age between 17 to 45 years old can be described as the follows: the number of the offenders of the age between 17 to 25 is 41, the number between 26 to 35 is 39, and the number between 36 to 45 is 21, constitutes 27 percent, 26 percent and 17 percent of all of the reported offenders (including the offenders whose ages are non-available) separately. In the age group of 17 to 45 years old, 17 to 25-year-olds constitute 40.6 percent, 26 to 35-year-olds 38.6 percent, and 36 to 45-year-olds 20.8 percent separately. The ratios of offenders seem to be decreasing with age.

3. Domestic versus foreign perpetrators

Altogether 14 out of 115 cases were committed by international perpetrators or foreigners, a ratio of weaker than 12.2 percent. Domestic perpetrators are responsible for the rest 87.8 percent of the cyber criminals. Majority of the reported cases are domestic computer offences.

4. Insider versus outsider

Insiders and outsiders constitute different ratios in different categories of

offences. The categories in which the insiders constitute the majority of offenders include: all offenders of data theft and espionage were insiders, while 57.1 percent of fraudsters are insiders.

The categories in which outsiders constitute the majority of offenders include: exactly 100 percent of ID theft, approximately 92.9 percent of miscellaneous (including embezzlement and corruption), approximately 87 percent of attack and sabotage, approximately 81.8 percent of viruses, worms, spyware and logic bomb, and approximately 76.2 percent of hacking and sabotage. In fact, outsiders also constitute a strong ratio in fraudsters: approximately 42.9 percent.

The former employees are included in the category of outsiders. A significant ratio of offenders of attack and sabotage are former employees, who constitute approximately 43.5 percent. Former employees also constitute 12.7 percent of offenders of hacking and illegal access, and approximately 7.2 percent of offenders of embezzlement and corruption.

Overall, insiders and outsiders constitute 21 percent and 79 percent of all reported offenders separately. The former employees constitute 16 percent of all of the outsiders. If add up former employees into insiders, they would constitute about 34 percent of the total offenders, still a less ratio than outsiders.

5. Losses of cybercrime

In more than 59 percent of cybercrime cases, no loss was mentioned in the report. Among the rest less than 41 percent of cases, approximately seven percent are with losses less than 10 thousand dollars, approximately 15.7 percent with losses between 10 thousand and 100 thousand dollars, approximately 10.4 percent with losses between 100 thousand and one

million dollars, and approximately 9.6 percent with losses more than one million dollars.

Hacking and illegal access, viruses, worms, spyware and logic bomb, ID theft, and miscellaneous (including embezzlement and corruption) are among the top list with most average losses, each of which are beyond one million dollars. The average losses of attack and sabotage, data theft and espionage, and fraud are relatively lower, 160 thousand, 5 thousand and 384 thousand dollars separately.

Overall, the average loss of the reported 49 cases with is more than 2.989 million dollars. Adding cases without losses reported, the average loss still reaches 1.274 million dollars.

6. Victims of cybercrime

Private sector is the primary victim of cybercrime. All of the cases of data theft and espionage, ID theft, and fraud are against private interest. Approximately 87.5 percent of miscellaneous (including embezzlement and corruption), approximately 81.8 percent of viruses, worms, spyware and logic bomb, approximately 77.3 percent of attack and sabotage, approximately 69.5 percent of hacking and illegal access are committed against private sector.

Only approximately 18.2 percent of attack and sabotage, approximately 13.6 percent of hacking and illegal access, and approximately 12.5 percent of miscellaneous (including embezzlement and corruption) are against public sector.

Besides, approximately 15.3 percent of hacking and illegal access, and approximately 9.1 percent of viruses, worms, spyware and logic bomb

cases are against both private and public sectors.

In addition, approximately 9.1 percent of viruses, worms, spyware and logic bomb, approximately 4.5 percent of attack and sabotage, and approximately 1.7 percent of hacking and illegal access cases are against public health and safety, as it was named.

7. Guardianship level of the victim

In majority of cases, the guardianship is weak. Exactly 100 percent of cases of data theft and espionage, and ID theft are possibly due to the absent of related guardianship. In other cases, approximately 90.9 percent of viruses, worms, spyware and logic bomb, approximately 87.5 percent of miscellaneous (including embezzlement and corruption), approximately 82.6 percent of attack and sabotage, approximately 80 percent of fraud, and approximately 74.6 percent of hacking and illegal access are due to weak guardianship.

Approximately 20 percent of fraud cases, approximately 16.9 percent of hacking and illegal access, and approximately 9.1 percent of viruses, worms, spyware and logic bomb could be classified into the category of medium guardianship.

Only approximately 17.4 percent of attack and sabotage, approximately 12.5 percent of miscellaneous (including embezzlement and corruption), and approximately 8.5 percent of hacking and illegal access could be stated as with strong guardianship, even though the offences are succeeded.

8. Complexity of cybercrime

All the cases of data theft and espionage seem uncomplicated to perpetrate. Approximately 87.5 percent of miscellaneous (including embezzlement and corruption), approximately 80 percent of fraud, approximately 73.9 percent of attack and sabotage, 66.7 percent of ID theft, and approximately 66.1 percent of hacking and illegal access involved no complicated techniques, or techniques that could be available most common computer or network users at the time of committing such offences.

Approximately 27.3 percent of viruses, worms, spyware and logic bomb, approximately 20 percent of fraud, approximately 12.3 percent of hacking and illegal access, and approximately 8.7 percent of attack and sabotage cases are committed with a medium level of techniques.

Cases of viruses, worms, spyware and logic bomb might involve the most complicated techniques, with 72.7 percent of which classified into the most complicated category. Approximately 33.3 percent of ID theft, approximately 18.3 percent of hacking and illegal access, approximately 17.4 percent of attack and sabotage, and approximately 12.5 percent of miscellaneous (embezzlement and corruption) might involve complicated techniques, or techniques unavailable to common users at the time of committing such offences.

9. Imprisonment sentences

The punishments for many cases are labeled with “to be decided.” The study calculated the punishment of the sentenced cases. The average imprisonment for the data theft and espionage case is 50 months, the longest among all the categories of cybercrimes. Attack and sabotage, and

miscellaneous (embezzlement and corruption) are imposed the same average imprisonment of 40.3 months. Fraudsters obtained an average imprisonment of 32.5 months. Attack and sabotage cases are sentenced with an average imprisonment term of 28.1 months. The shortest average imprisonment term, 21.9 months, is imposed on hacking and illegal access perpetrators, that is, the hackers.

Total imprisonment term imposed on reported 53 offenders is 1429 months, with an average of shorter than 27 months. Among these cases, the longest imprisonment is 96 months, while the shortest is only one month.

10. Fine sentences

Fine is usually imposed on perpetrators of hacking and illegal access, and attack and sabotage. Overall, exactly ten cases ended with fine of lower than 10 thousand dollars, nineteen cases with fine between 10 to 100 thousand, twelve cases with fine between 100 thousand and one million, and two cases with fine over one million dollars (one case fined 2 million and the other case fined 7.8 million dollars).

The fine imposed on offenders 43 offenders totaled 13.45 million dollars, with an average of 312.78 thousand dollars. However this sum is greatly due to the high fines in two cases where the offenders were fined with 2 and 7.8 millions dollars, which contribute to an average of 228 thousand dollar for each case calculated. Except these two cases, the average fine of the 41 cases is approximately 89 thousand dollars.

Discussion and conclusion

The subjects of cybercrimes can be either insiders or outsiders. Many studies found that the insiders constitute a great threat to the employers' systems. However, younger juveniles might be less employed than older juveniles. That is to say, the younger juveniles may represent the increasing outsiders engaged in cybercrimes. On the other hand, the nature of cybercrime decides that the perpetrators do not have age limit. Any one who can use the computers and Internet can commit cybercrime.

In my opinion, the concept of white-collar crime could not fit the situation of cybercrime. Although the white-collar crime emphasizes the employment and social status of the criminals, I consider that one of the most relevant factors in white-collar crime is the knowledge that the criminals have acquired from both their pre-employment education and their occupational career. It is not oversimplified to view white-collar crime as a knowledge-based offence, compared with violence-based traditional offences. Different from either of these two kinds of conceptions, cybercrime could be either knowledge-based white-collar crime or knowledge-based cyber violence. Overall, there is a reluctant distinction between cybercrime, white-collar crime and even violent crime.

However, it is reasonable to conclude that, when there were few computers, the employees in the computer-related industries were among the small number of computer users. They acquire more chances to conspire an offence against their employers. With the prevalence of personal computers and the development of the Internet, the insiders remain to keep their advantages in having a better knowledge about the access control mechanisms, assets management systems, and the overall loopholes. The insider knowledge, convenience, and directness encourage

the employees to commit cybercrimes. As the United States Secret Service and CERT Coordinator Center's study disclosed that minimal technical skill was required in launch cyberattacks on banking and finance sector (Randazzo and co-workers 2004).[5]

In addition, insiders are exposed them to the negative psychological influence derived from their information work environment. Shaw, Ruby and Post (1998) identified the characteristics that increase the tendency towards illegitimate and harmful conducts of the employees, including computer dependency, a history of personal and social frustrations (especially anger toward authority), ethical flexibility, a mixed sense of loyalty, entitlement, and lack of empathy.

On the other hand, the offences by the insiders involve less complicated process of being traced, detected and investigation than that by the outsiders. If we could not judge whether insiders or outsiders are liable for more cybercrimes, we should firstly consider the question on who are more possible to do it and who are more possible to be caught. The insiders surely coincide both of the situation. Furthermore, it is more efficient for the law enforcement to reveal an inside misuse than an outside attack, they are rationally more likely to pay more attention to the current and previous employees. The outside incidents or international disturbances would possibly be disregarded at the first sight of the investigation, except it deserves an international show-off.

Summarily, the study found that males are responsible for a majority of cybercrime. The cybercriminals distribute primarily among the ages between 17 to 45 years old. Domestic perpetrators constitute the absolute majority of the cybercriminals. Outsiders are four times more likely to be involved in cybercrimes than insiders. A large part of the cybercrimes did

---

[5] In different studies, the term insider is defined differently. In Randazzo and co-workers (2004), insider was defined as including "current, former, or contract employees of an organization."

not cause economic loss. However, once involving losses, the average sum could reach as high as one million. The primarily endangered interests are of private sector, even though the threats to the public sector have usually been given more concern. The guardianship of the victims is surprisingly weak, vulnerable to the uncomplicated cybercrimes. The punishments (both imprisonment and fine) against cybercrime are generally light.

The limit of this study is that the sample cases are randomly selected published on the United States of America Department of Justice web site. They could be regarded as typical cybercrime cases, but it is difficult to say whether they could be considered the representatives of the cybercrimes happened in the United States. Therefore, this study is an explanation on the cases as "they are." Sample survey is usually used to give a sketch for the scenario of the whole through the part, but this study warns careful generalization of its findings to the related items of all the cybercrimes. To avoid the shortcomings in the materials, the ideal study should cover a random sample in a wider range of cases, if it is available.

References

1. Becker, J. Who Are the Computer Criminals, *Security Management*, January 1981, pp. 18-20.
2. Bequai, August. *Computer Crime*, Lexington, Massachusetts, Toronto: Lexington Books, 1978.
3. Dong, B. Eighty Percent of Net Café Consumers Are Youths, *China Youth Newspaper*, 15 October 2003.
4. Howitt, Dennis. *Forensic and Criminal Psychology*, Essex,

England: Pearson, 2002.

5. Jiang, Ping. *A Study on Computer Crime*, Commercial Printing Company, 2000, pp. 151-152.
6. Levinson, D. (ed.) *Encyclopedia of Crime and Punishment*, Newbury Park, CA: Sage Publications, 2002.
7. Mackenizie, E., and Goldman, K. Computer Abuse, Information Technologies and Judicial Affairs, in *Proceedings of the 28th Annual ACM SIGUCCS Conference on User Services: Building the Future*, 2000, pp. 170-176.
8. Meta Group. Security Spending Spree, *PC Magazine*, 20 January 2004.
9. Nelson, M. Internet Security Systems' Chris Klaus Says Companies Should Close Back Doors to Be Secure, *InfoWorld,* 10 January 2004.
10. Nordic Council of Ministers, *Nordic Information Society Statistics 2005, TemaNord 2005:562.* Copenhagen: Nordic Council of Ministers, 2005.
11. Parker, D. B. *Crime by Computer*, Charles Scribner's Sons, New York, 1976.
12. Randazzo, Marisa Reddy, Keeney, Michelle, Kowalski, Eileen, Cappelli, Dawn, and Moore, Andrew. *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector,* Carnegie Mellon Software Engineering Institute, August 2004.
13. Reynolds, George. 2003. Ethics in Information Technology, Thomson Course Technology.
14. Shannon, L. R. The Happy Hacker, *New York Times*, 21 March 1993, p. 2.

15. Shaw, Eric D., Ruby, Keven G., and Post, Jerrold M. The Insider Threat to Information system, *Security Awareness Bulletin*, number 2-98, September 1998.

16. Sinrod, E. J., and Reilly, W. P. Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, *Computer and High Technology Law Journal*, volume 16, May 2000, pp. 177-232.

17. Syngress. *Scene of the Cybercrime: Computer Forensics Handbook*, Rockland, MA: Syngress Publishing, 2002.

18. Underwood, Jim. Criminal Profile, 16 October 2002. Retrieved 8 July 2006, from http://www-staff.it.uts.edu.au/~jim/cit2/cit2-99/legal/CrimProf.html

19. Vatis, M. A. *Congressional Statement, Federal Bureau of Investigation, National Infrastructure Protection Center (NIPC) Cyber Threat Assessment, Before the Subcommittee on Technology and Terrorism of the Senate Committee on the Judiciary*, 6 October 1999.

20. Ware, H. W., Pfleeger, C. P. and Pfleeger, S. L. *Security in Computing, Englewood Cliffs*, New Jersey: Prentice Hall PTR, 2002.

21. Wasik, Martin. *Crime and the Computer*, Oxford: Clarendon Press, 1991.

CHAPTER V CYBERSTALKING

Introduction

In my research on motives for cybercrime, I conclude that curiosity is an overwhelming psychological power, propelling people to identify the unidentified and to manage the unmanageable, or to demolish the established, and to deorganize the organized, whether in the macro or the micro dimensions. Information systems are a dimension which has developed to some extent under the dynamics of human curiosity and has been threatened to some extent by this force (Li 2008, p. 198).

Curiosity propels people to acquire new knowledge on things around us. People are always curious for good, or curious for bad. Observing is a process of people acquiring fresh understanding from outside world. With the progress of civilization, objects of observing can range from material world to spiritual world, from macroworld to microworld, and from environment to human beings and fauna and flora. Everybody was growing in all conscience obtain perception and dexterity by perpetually observing. Even when the observed person became unwilling and unhappy to be observed, observation could hardly be suspected, prevented, or

denounced. Conflicting are motives of those who want to reveal and that of those who want to conceal. When the observed became fearful and distressed that their or their family members' health, wealth, privacy and spiritual welfare are prone to suffer losses due to nettlesome observing, they perceive a parlous stalking. Thence observation was classified into at least two categories: wanted harmless observation and unwanted harmful observation. As a matter of fact, stalking has long been a known activity of an obsessive stalker towards a distressed stalkee. Although stalking might have had a long history, its impact attracted broad attention in recent several decades.

Stalking can be defined in a mixture of ways. This article is not intended to engage in disputation on issue of definitions, even though many authors may not agree with each other, or agree with the way by which this article deals with the definition question, the effect of which was too often overestimated by too many authors. Wikipedia can be edited by professional or amateur authors, comprehensively defining stalking as "the obsessive following, observing, or contacting of another person, or the obsessive attempt to engage in any of these activities, including following the person to certain places, to see where they live or what the person does on a daily basis, it also includes seeking and obtaining the person's personal information in order to contact him or her (2008a). Many writers claim that there is hardly a consensus on how to define stalking, in practice, from existing literature, it is clear that there is hardly any dissension on its fundamental aspects. Of course, if it is to make some particular comparison for the purpose of defining it more precisely, differences can be found between them. Yet the character, occurrence, and impact of stalking are only currently being systematically studied (Mullen and Pathe 2002, p. 273), and legislation has not been prepared until 1990 in main western countries (Spitzberg and Hoobler 2002, pp. 71-72).

It seemed that shortly after traditional stalking had been criminalized, new approaches for stalking emerged as the adoption of some high technological inventions were used in monitoring people's activities. In the end, what happened that made stalking a public concern by such new technologies? Some insist that cyberstalking has developed from traditional stalking, while others claim that it is completely different. Based on the recognition of stalking as a kind of long-existing human-human observation, this article will expatiate on recent development that can be expressed as from traditional stalking to cyberstalking by presenting particular power of the Internet and search engines. Cyberstalking is the exploitation of information and communication technological methods to follow other persons repetitively to cause displeasure, annoyance, distress and fear. In essence, cyberstalkers exploit information and communications technology, particularly the Internet to harass another individual, group of individuals, or organization, including false accusations, monitoring, the transmission of threats, identity theft, damage to data or equipment, the solicitation of minors for sexual purposes, and gathering information for harassment purposes (Wikipedia 2008b). This article will consider a conceptual dilemma revolving around the limit between acceptable observation and unacceptable stalking, through reading of a few cases and laws. This article will also consider an emerging phenomenon that stalking is being socialized through the pervasion of online social network services.

The Internet makes stalking different

The development of information and communications technology (ICT) is

powerful, bringing it with omnifarious opportunities for individual and enterprise users. Indicators such as growth of the number of personal computers and Internet users, the increase in the number of web sites, Internet hosts and web pages, bandwidth growth, the growth of scale of e-commerce and e-governance demonstrate the essential reality of development (Li 2008, pp. 82-89). Neither people connected through information system might necessarily be as good as within a Weberian formally rational regime, nor as bad as in a Hobbesian "war of all against all", nor as ideal as Platonian *Republic*, and Moresian *Utopia* (Li 2006d). To understand the essence of cybersecurity, we must hold a standpoint of a relative concept (Li 2006a; Li 2006b). Vulnerabilities of the information society impend over the horizon of society's aspiration to an affirmative prospect (Li 2008, pp. 89-111). Cyberinsecurity and cybercrime impose new work load on people thinking about welfare of this generation (see Li 1992; Li 1994; Li 2006a; Li 2006b; Li 2006c; Li 2006d; Li 2006e; Li 2007a; Li 2007b; Li 2008).

Internet services, such as e-mails, are also abused by cyberstalkers to send text-, graphic-, audio- and video-based messages to the e-mail account of the intended victim, transmitting the content of threatening, alarming, or harassing (D'Ovidio and Doyle 2003, pp. 10-17). Other Internet services can also be exploited by cyberstalkers to harass other users, either directly or indirectly. An example of direct harassment can be found when stalker sends harassing messages to a targeted victim. An example of indirect harassment can be found when a stalker uses the Internet communications to obtain a potential victim's personal information, such as a home address etc., and then uses the information to contact by other means (Internet Crime Forum IRC subgroup 2001, p. 11).

Behind all the good that information and communications technology does to contemporary society, victims of stalking have been confronted

with a lugubrious process of cyberization. With the increase of Internet users, web sites, Internet hosts, web pages, bandwidth, and the growth of e-commerce, society is transiting from the process of urbanization to cyberization, taking shape an information supercontinent. The increasing significance of the Internet for society and the accumulated threats of abuse draw widespread consideration (Li 2008, pp. 82-89). People are stymied by their increasing dependence on information and communications technology as the solely dominant instrument in their routine activity. Unimaginable consequences are possible when abuse and crash of the systems occur. Cyberization makes it easier for stalkers to have access to more victims, to exhibit more pestering by more means, through more routes and in broader spatial distribution, to repeat more times of same nuisance, to last for a longer span of time of harassment, and to cause more serious ill effects. Cyberized stalking threatens a great population of netizens, who in turn cannot get rid of such harassment by merely moving from one country to another, or by disconnecting him/herself from the Internet.

Stalking can be one of the examples of uncontrollable networked activities, engendered by many factors characterizing the cyberspace. Universal access to the networked information systems can have both constructive and unconstructive characters in terms of social development and social control. Constructive, for the reason that the society is regrouped by the networks, which are accessible for larger number of societal members. Unconstructive, for the reason that the traditional social networks have been substituted and the members are migrating to and participating the construction of new networks (Li 2008, p. 91). The powerlessness of the old order and the deficiency of the new order will generate an integration vacuity, to be articulated in the appearance of disorder and confusion, for a course of disintegration and disorganization

can be foreseen during this change (see Mowrer 1942; Elliot and Merrill 1961). Potential cyberstalkers can be placed under weaker surveillance while potential stalkees can be placed under weaker protection in cyberspace than in meat space. In Cullen v White [2003] WASC 153 (3 September 2003), the defendant originally published a number of postings in a discussion forum on the World Wide Web, disparaging of a university where the plaintiff once worked and a number of people whom the plaintiff had known there. After the plaintiff had known this, he wrote to the webmaster to urge him to remove the postings. The webmaster published the plaintiff's letter on the discussion forum web page. Within days the university where the plaintiff was then studying, began to receive e-mails from the defendant claiming that the plaintiff was a fraud. Within two months, the defendant had created a web site for his attacks on the plaintiff. The cyberspace armed the defendant with electronic bombardment of fake accusations about the victim.

Conventional countermeasures and theories about crime prevention were based on its material influence and on the material environment, although non-material factors have long existed, too. Cyberspace is developed from information systems as an abstract space, differing from the material devices of information systems that include terminals and cables. It is invisible and intangible if compared with traditional space (Khosrow-Pour 1998, p. 440; Robertson 2000, p. 248; Dodge and Kitchin 2001, p. 81). Stalking occurring in cyberspace leaves no directviewing traces except electronic traces, causes no directviewing effects except digitalized effects, and leads to no directviewing detection except through computerized detection. Yet it harms the victim living in the real space.

In addition, the process of online stalking has low controllability. Since the early days of invention and use of the computer and the Internet, insufficient efforts have been made to exercise control over

conducts facilitated by them. Thus the idea of control over the Internet has been located in an extremely embarrassing position:

"The Internet can be controlled by any of the users if there is anyone trying to exercise control over part of it; but it cannot be controlled by any of the users if they want to exercise absolute control over the whole system. The low controllability by one means, on the other hand, the high possibility of control by many others. The low controllability by authorized users means the high possibility of control by unauthorized uses." (Li 2008, p. 94)

"The impossibility of control over the Internet immunizes individuals and institutions from any liability for the omission of such a control. Under these circumstances, neither an ex ante obligation nor an ex post liability can be adhered to as far as related individuals and institutions are concerned. Thus the incentive for control will hardly be strong." (Li 2008, p. 96)

From Cullen v White, we can see that once stalking takes place, the victim's wish of stopping the spread of the false accusations becomes problematic before they are clearly identified, conflicting the popular position of free information and the legal orientation of free speech.

Data processed and transmitted via information systems can also be of low confidentiality. In principle, it is required that protected data in information systems be "obtained and processed fairly and lawfully"(Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 5; Directive 95/46/EC, Article 1 (a)). Technical and organizational measures should be taken to protect personal data against access without authorization, manipulation, disclosure, transfer and other processing without legal reason. Besides general protection of personal data, sensitive personal data are granted

special safeguard by law. Information systems are usually analogous to a place with unrestricted freedom and where the information is less confidential. Weak technical control and weak human control are the main factors that expose the weakness of the systems (Li 2008, pp. 100-102). Under such circumstances, information about netizens can easily be pried and subsequently exploited by potential stalkers, not to mention general hackers.

Furthermore, anonymity in cyberspace does also matter. The real identity of the user is not necessary for using the Internet. In the environment of online communications, particularly during interaction between remote strangers, information systems provide the possibility of maintaining anonymity, and we found that the users of information systems have the willingness to stay passively anonymous, not necessarily actively lying to their counterparts (Li 2008, pp. 103-105). In the case of stalking, a stalker can sedulously conceal his/her identity while revealing or using the victim's. In USA v. Erik Bowker (United States of America, Plaintiff-appellee, v. Erik Bowker, Defendant-appellant, United States Court of Appeals (Sixth Circuit. - 372 F.3d 365, Submitted: March 10, 2004 Decided and Filed: June 11, 2004), during over one year, the stalker sent a number of emails full of verbal threats relating to the victim. The emails were sent from several different email addresses and purported to be from an individual variously identified. After an FBI Special Agent sent emails to the various email addresses on the correspondence pertaining to the victim, the victim began receiving hand-written notes from a person of different identity almost every couple of days. Even worse, after the victim more to a new location, the stalker, with different identities, sent the victim a card saying that his letters to her were all online in a mail account at yahoo.com. The stalker also continued to attempt telephone contact with the victim, 146 telephone calls from his cell phone to where

the victim worked and 16 calls to the victim's personal residential telephone. Knight's number was unlisted and unpublished. While the stalking was continuous and obsessive, the identity of the stalker reserved changed and concealed, taking FBI agent several months to trace back.

It is necessary to point out that, anonymity does only not cost the victim and law enforcement, but also cost the perpetrator. As Ariz. Rev. Stat. § 13-2921 provides that, if a person anonymously or otherwise contacts, communicates or causes a communication with another person by verbal, electronic, mechanical, telegraphic, telephonic or written means in a manner that harasses, his/her act constitutes the offence of harassment (see also Ala. Code § 13A-11-8 (b)(1)a).

The Internet and the World Wide Web enable to broadcast false accusations and induce third party harassment. The stalker might publish malicious postings to MySpace, Facebook, Craig's List and other Internet social sites, disclosing the stalkee's personal identity information. In one case, a stalker posed himself as the stalkee and distributed Web site invitations to visit her residence for sexual gratification (Office of the United States Attorney Western District of Missouri John F. Wood 2008). Here the stalker did harms to the victim through the hands of many others. Information and communications technology enables abundant methods for spreading malicious usually falsified messages using falsified identity. In order to prevent and deter similar stalking, newly implemented laws usually criminalize act of "causing a communication with another person by verbal, electronic, mechanical, telegraphic, telephonic or written means in a manner that harasses" (Wyo. Stat. § 6-2-506 (b)(i)).

From above discussion, a natural conclusion can be drawn that new technologies are making detection of stalking harder while making operation of stalking easier.

Human flesh search engine: enabling the unable

Stalking without the Internet and stalking with the Internet can have similar effects. In R. v. Goll (Gill, R v [1998] EWCA Crim 1061 (24th March, 1998), No: 97/5998/Y4), the stalker wrote eight letters to the victim, containing both threats and expressions of the way the stalker felt attracted to her, causing her and her family a great deal of stress and anxiety. The same stalker also sent 65 letters to another victim in the same way.

Cyberstalking, involving the repeated and persistent attempt by one individual, the stalker, to harass another individual, the victim, using the Internet or other open network (Burmester, Henry and Kermes 2005), can produce the same effect as this traditional one. Nonetheless, cyberstalking can have many different characteristics.

Stalking firstly means collecting information about somebody and his/her whereabouts. Down the ages, process of information collection becomes increasingly straightforward. In USA v. Devon Lynn Townsend (Cr. No. 07-CR-1363-WJ, Document 20. Filed 06/29/2007), during 11 months, the defendant from New Mexico used an interactive computer service, and a facility of interstate commerce to engage in a course of conduct that caused substantial emotional distress to Mr. and Mrs. Chester and Talinda Bennington in California (pp. 5-6). Over the course of several months, the defendant was able to access all sorts of private information about the Benningtons from their private e-mail accounts, including:

"(a) family pictures of the Benningtons and their minor children;

(b) correspondence between Wamer Brothers Records and the business attorney for Linkin Park, including a copy of a check made payable to Chester Bennington from the record company as well as a copy of the recording contract between Wamer Brothers Records and the members of Linkin Park;

(c) information about a new home purchase by the Benningtons which included such documents as a home inspection report, images of the home's interior, and other real estate documents;

(d) information about the Benningtons' travel plans including flight information and the name of motels and hotels where the Benningtons had reservations;

(e) a copy of a dental bill for Talinda Bennington;

(f) information about the time and location of Mrs. Bennington's childbirth classes;

(g) e-mail correspondence concerning the whereabouts and after school activities of the Benningtons' child;

(h) information about purchases the Benningtons made for their newborn child;

(i) information about the schedule and itinerary of the members of Linkin Park, including their itinerary for the Grammy awards show in 2006" (pp. 7-8).

It is surprising that these items of information can be obtained through the powerful function of search engine, which is termed "renrou sousuo yinqing" in Chinese (literally meaning human flesh searching engine in English). The power of "renrou sousuo yinqing" does not come from anything distinct from existing search engines, but from mobilizing hundreds, thousands or millions of Internet users to participate in, to

concern, to search, to contribute their findings, and even to track down all the way into target person's company, family, house, car, mobile phone, e-mail account and other online identity. In many published cases, human flesh search mobilization has positively assisted to identify deviants in a more efficient way. It should be considered valuable for law enforcement to reasonably develop and use such an approach. At the same time, many people are worried about issues such as disclosure of personal privacy. As far as malicious search is concerned, human flesh search engine can be abused in stalking and harming a benign party, or a party that his/her deviant behaviour should not be publicised as in such details.

Usually, traditional and electronic methods are incorporated in real-life stalking. The Internet provides stalkers with either primary information or complementary information about the stalkee. For example, in Johnson, R (on the application of) v DPP ([2005] EWHC 3123 (Admin) (08 December 2005)), the stalker used direct harassment, consisted of silent telephone calls at work, home and on the victim's mobile phone; following her, appearing by the classroom and in the car park; following her in his car, causing her to feel scared and threatened; following her, swerving in front of her and braking sharply, in order to prevent her getting past; trying to drive her off the road. The stalker searched home addresses of various people called the same name as the stalkee. There was also indirect harassment, consisted of a barrage of letters to the victim's employers questioning her professional conduct and fitness to teach and causing internal investigations to take place. The conduct here belongs primarily to traditional stalking, but there is also the element of cyberstalking.

The incorporation of stalking and cyberstalking can well illustrate the similarities and differences between them, and sketch the evolution process of deviant behaviours.

Information and communications technology created, inter alia, convenience for forming of large online social networks, which are facilitated by websites specialized on so-called social network services. Social network services convoke groups of people who have common experience, or share common interests, or even participate in common activities. Currently, primary social network services are provided by websites such as MySpace, Facebook, Friendster, Hi5, etc. Emerging social networks can be viewed as a double-edged sword, granting curious users greater freedom of information access on the one hand, while bringing about more threats to unprotected netizens on the other. Indeed, online social network services change traditional stalking into a socialized lethal weapon: collective stalking, organized stalking, industrialized stalking, and worldwide stalking become a near reality.

Searching or stalking: an ambiguous limit

It is necessary to discuss an issue related to how people think about information about them. Some information can have greatly different status in different cultures, different industries, and different uses.

The sensitivity of different aspects of personal information differs from one (sub)culture to the other. For example, the status of information about one's age can range from absolutely public to absolutely private. When people meet in rural Northern China, it is a usual practice that people exchange information about each other's name, age and family members. There is hardly any taboo subject from information about their personal, family and professional information, including, for example, inability, salary, residence, and so on. Here, age is public. But in many

other cultures, age is more or less a taboo, asking one's age being a coarse-grained behaviour. As a result, people from a culture that holds age public making every attempt to ask one's age from a culture that holds age private may well be defined as a kind of stalking.

With search engine, it is very effortless to find a set of personal information about someone you are unfamiliar with, particularly, about celebrities. Often times, such information can be as detailed from their sex, age, education, current profession, work experience, hobbies and interests, places visited, articles and books published, conferences participated, or even residence, and their family members' sex, age, education and profession. Such information can be collected by various "fans", or provided by people themselves. In USA v. Devon Lynn Townsend (Cr. No. 07-CR-1363-WJ, Document 20. Filed 06/29/2007), the defendant has been a fan of the alternative or nu metal band Linkin Park, for which the stalkee Chester Bennington is the lead singer, and Talinda Bennington is Chester Bennington's wife (p. 6). He learned a lot through the Internet about Chester and Talinda Bennington. After he gained unauthorized access to a server of yahoo.com, he hacked into Chester Bennington's personal e-mail account, being able to review and download all of Mr. Bennington's private e-mail correspondence there, and to find out about Talinda Bennington's e-mail address from accessing her husband's account (pp. 6-7).

Professor is in no way a star-like profession, yet occasionally some of them disclose their personal information in details as those stars do. Their original intention may be to relate such information to their academic proposition and they think their information will interest anyone other than colleagues and students. Transmitted from academic circles to other communities, however, such information can become source of stalking.

Sometimes, personal information is published on some media for

public use, such as telephone directory, which usually collects names, profession, telephone numbers, residence addresses, websites, and even e-mail accounts. Publishing such information means users of this directory can make telephone calls, write letters or e-mails, visit homepages, and even pay visits in person to them. Disputation does not occur about the legal nature of using public information, but occurs about who can, at what time, how frequently, and for what purpose one can use such information. Such disputation is involved particularly when it happens that difficult is to judge whether an act is normal use or abnormal use of contact information. Some stalking laws and cyberstalking laws give unique answers to provide constituents of the tort or the offence. For example, Australian Capital Territory Crimes Act 1900 s34A (see also Northern Territory Criminal Code Act 1997 s189 (1), Queensland Criminal Code Act 1899 s359A (7), South Australia Criminal Law Consolidation Act 1935 s19AA (1)(a), Victoria Crimes Act 1958 s21A (2)) provides that stalking shall be constituted, on at least two occasions, the stalker

"(a) follows or approaches the other person;

(b) loiters near, watches, approaches or enters a place where the other person resides, works or visits;

(c) keeps the other person under surveillance;

(d) interferes with property in the possession of the other person;

(e) gives or sends offensive material to the other person or leaves offensive material where it is likely to be found by, given to or brought to the attention of, the other person;

(f) telephones or otherwise contacts the other person;

(g) acts covertly in a manner that could reasonably be expected to arouse apprehension or fear in the other person; or

(h) engages in conduct amounting to intimidation, harassment or molestation of the other person." (subsection (2))

And with intent to cause the following effect:

"(a) apprehension or fear of serious harm in the other person or a third person; or

(b) serious harm to the other person or a third person." (subsection (1))

It is also easy to find in stalking laws the clear illumination about the subjective aspect. New South Wales Crimes Act 1900 s562AB provides that "a person intends to cause fear of personal injury if he or she knows that the conduct is likely to cause fear in the other person." (subsection (3), see also South Australia Criminal Law Consolidation Act 1935 s19AA (1)(b), Victoria Crimes Act 1958 s21A (3))

Queensland Criminal Code Act 1899 s359A clarifies the objective and subjective aspects of the offence. Besides, the merit of this law is that it establishes a prerequisite the offence of stalking to be constituted that the potential stalkee be aware of the stalking is directed at the him/her, hence he/she can (subsection (1)(c)). This law might have clarified another significant aspect about stalking by excluding the course of conduct engaged in for the purposes of a genuine industrial dispute, or political or other public dispute or issue carried on in the public interest (subsection (4)). Victoria Crimes Act 1958 s21A (4) detailedly lists exceptions by pointing out conduct engaged in by a person performing official duties for the purpose of the enforcement of the criminal law, the administration of any Act, the enforcement of a law imposing a pecuniary penalty, the execution of a warrant, or the protection of the public revenue. Ala. Code § 13A-11-8 (b)(1)b. generalizes such a prerequisite as an act (that is making a telephone call) "with no purpose of legitimate communication".

However, the drawback of a provision in Queensland Criminal Code Act 1899 s359A is located in its subsection (2)(b), which provides that "the first person intends that the second person be aware that the course of conduct is directed at the second person, even if the concerning acts or particular concerning acts are done to, or to the property of, a person other than the second person." The clause blurs the natures of a harassing conduct of a person who deliberately makes the stalkee aware of the conduct and a harassing conduct of a person who deliberately makes the stalkee unaware of the conduct.

Clarification of another possible misgiving about the constitution of stalking may refer to Alaska Stat. § 11.41.270 (b)(3), which provides a definition for "nonconsensual contact", as "any contact with another person that is initiated or continued without that person's consent, that is beyond the scope of the consent provided by that person, or that is in disregard of that person's expressed desire that the contact be avoided or discontinued."

Conclusion

Exploiting new technological methods, cyberstalking poses severe intimidation to netizens who are told that cyberspace could enable them many things, fast and efficiently, in the information age. Shortly after traditional stalking had been criminalized, new approaches for stalking emerged as the adoption of some high technological inventions were used in monitoring people's activities. Based on the recognition of stalking as a kind of long-existing human-human observation, this article expatiates on recent development that can be expressed as from traditional stalking to

cyberstalking by presenting particular power of information and communications technology and search engines. This article considers an emerging phenomenon that stalking is being socialized through the pervasion of online social network services. Generally, information and communications technology makes stalking prevalent, serious, ubiquitous, and socialized. The article discusses the limit between reasonable use of information and legal constitution of stalking.

References

1. Burmester, M., Henry, P. and Kermes, L. S. 2005. Tracking Cyberstalkers: a Cryptographic Approach, *Computer & Society Magazine*, ACM SIGCAS, 35(3-4), September 2005.
2. D'Ovidio, R., and Doyle, J. 2003. A Study on Cyberstalking: Understanding Investigative Hurdles, The FBI Law Enforcement Bulletin, volume 72, pp. 10-17.
3. Dodge, Martin and Kitchin, Rob. 2001. Mapping Cyberspace, New York, New York: Routledge.
4. Elliot, Mabel A. and Merrill, Francis E. 1961. Social Disorganization, fourth edition, New York, Evanston, and London: Happer and Row Publishers.
5. Internet Crime Forum IRC Subgroup. 2001. Chat Wise, Street Wise-Children and Internet Chat Services.
6. Khosrow-Pour, Mehdi. 1998. Effective Utilization and Management of Emerging Information Technologies, Hershey: Idea Group Publishing.

7. Li, Xingan. 1992. Jisuanji Fanzui Xingfa Shiyong Wenti Chutan (Exploration into Issues of Application of Criminal Law to Computer Crime), Yanjisheng faxue (Graduate Law Review), Issue 3 (in Chinese).

8. Li, Xingan. 1994. Jisuanji Fanzui Ruogan Wenti zhi Yanjiu (A Study on Several Issues in Computer Crime), China University of Political Science and Law, Beijing: China University of Political Science and Law, Master's degree thesis (in Chinese).

9. Li, Xingan. 2006a. Economic Analysis of Cybersecurity: The Mixed Provision of Private Good, in John Roufagalas, ed. Resource Allocation and Institutions: Exploring in Economics, Finance and Law, Athens, Greece: ATINER, pp. 607-620.

10. Li, Xingan. 2006b. Relative Concept of Cybersecurity, Information and Security: An International Journal, Volume 18, pp. 11-24.

11. Li, Xingan. 2006c. E-marketing, Unsolicited Commercial E-mail, and Legal Solutions, Webology, Volume 3, Number 1. Retrieved September 20, 2008, from http://www.webology.ir/2006/v3n1/a23.html

12. Li, Xingan. 2006d. Cyberspace and the Informed Rationality of Law, in Ahti Laitinen ed. Writings in the Sociology of Law and Criminology, University of Turku Faculty of Law.

13. Li, Xingan. 2006e. The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited through Typical Cases Prosecuted, University of Ottawa Law and Technology Journal (accepted in 2006, in press).

14. Li, Xingan. 2007a. International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene, Webology, Volume 4, Number 3. Retrieved September 20, 2008, from http://www.webology.ir/2007/v4n3/a45.html

15. Li, Xingan. 2007b. The Phenomenon of Unsolicited E-mails with Attachments, SIMILE: Studies In Media and Information Literacy Education, Volume 7, Number 2, May 2007, DOI 10.3138/sim.7.2.003, pp. 1-11.

16. Li, Xingan. 2008. Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society, Turku, Finland: Uniprint.

17. McFarlane, L. and Bocij, P. 2003. An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers, *First Monday*, Volume 8, Number 9. Retrieved August 8, 2008, from http://firstmonday.org/issues/issue8_9/mcfarlane/index.html

18. Mowrer, Ernest R. 1942. Disorganization: Personal and Social, Chicago, Philadelphia, New York: J. B. Lippinatt Company.

19. Mullen, P. E. and Pathe, M. 2002. Stalking, Crime and Justice, Volume 29, pp. 273-318.

20. Office of the United States Attorney Western Disctrict of Missouri John F. Wood. 2008. News Release, KC Man Indicted with Cyberstalking, May 9.

21. Robertson, Scott. 2000. The Digital City's Public Library: Support for Community Building and Knowledge Sharing, in Ishida, Toru and Isbister, Katherine eds. Digital Cities: technologies, Experiences, and Future Perspectives, Springer, pp. 246-260.

22. Spitzberg, B. H. and Hoobler, G. 2002. Cyberstalking and the Technologies of Interpersonal Terrorism, *New Media Society*, Volume 4, Issue 1, pp. 71-92.

23. Wikipedia. 2008a. Stalking. Retrieved August 8, 2008, from http://en.wikipedia.org/wiki/Stalking

24. Wikipedia. 2008b. Cyberstalking. Retrieved August 8, 2008, from http://en.wikipedia.org/wiki/Cyberstalking

CHAPTER VI UNSOLOCITED COMMERCIAL E-MAIL

Introduction

With the development of e-commerce and the prevalence of the Internet, e-mail has become the primary means of communications and marketing. Compared with the traditional marketing tools, e-mail has obvious advantages. However, the abuse of e-mail disturbs the normal communications services, and influences the environment for the public to use the Internet. The reception of unsolicited electronic messages and commercial information become a pervasive social and economic problem. The difficulties in identifying the senders and in compensating the recipients' losses further prove the uncontrollability of the Internet. Spamming impedes the effective application of telecommunications to the individual and business communication, baffles the consumers' acceptance of legal e-marketing, and in turn, hinders the growth of the e-commerce. Many individuals and institutions are making efforts to seek solutions to the problem (for example, Coalition Against Unsolicited Commercial Email, 1999; Cobb, 2003; Direct Marketing Association; Federal Trade

Commission, 1998, 2003; Ferguson & Piragoff, 1997; Gartner Consulting, 1999; Gauthronet & Drouard, 2001; Goodman & Rounthwaite, 2004; Hansell, 2003; International Telecommunication Union, 2004; Khong, 2001, 2004; Midnet Media, 2003; Mail Abuse Prevention System, 2004; Organization of Economic Cooperation and Development, 2003, 2004; Peppers & Rogers, 2000; World Summit of Information Society, 2003 and many others). In order to ensure the convenience of the Internet use and improve the security and efficiency of the Internet environment, some countries have implemented specific legislation to regulate spam; the European directives required the member states to incorporate commercial e-mail rules in the provisions on privacy and telecommunications. Organization of Economic Cooperation and Development (OECD) called for legislation and international cooperation in combating spam. Based on documentary analysis and empirical study, this Chapter explores the threats of the unsolicited commercial e-mail and the difficulties in dealing with the problem, analyzes the dilemmas in combating spam under the present legal framework, and suggests possible countermeasures.

Background and definition of spam

As the capability of computers and networks to process information increases, "a wealth of information" can lead to a "poverty of attention" (Simon, 1982). Unsolicited business e-mail (UBE) or unsolicited commercial e-mail (UCE) represents an example that e-mail users have to deal with the superfluous information they do not expect to consume. It is generally called bulk mail or spam. It turns out that spam has evolved into

a large amount of information garbage, polluting the environment of e-marketing. When we talk about the phenomenon of spam, we are talking about a negative externality in e-marketing that people try to get rid of. It brings about the negative image of e-marketing, frightening e-mail users from trusting the e-mail communications.

Up to April 2005, the population of global e-mail users increased to 683 million, with almost 1.2 billion lively accounts. The e-mail marketing has been regarded as one of the most successful marketing means on the Internet (Niall, 2000). Unfortunately, with the increase of the e-mail usage, two thirds of the total 130 billion messages sent and received everyday are unsolicited (Radical Group, 2005).

In nature, e-mails can be a kind of information goods, for example, messages provided by the paid subscription services; while at the same time, e-mail can also be a kind of bads, in case the subscribed paid information are harmful to general public or to specific groups or a certain person. If the information is provided free of charge, it becomes an externality. When the messages are useful, they are positive externalities; when they are harmful, they become negative externalities. Whether they are with charge or without charge is decided by the sender; but whether they are useful or harmful, is decided by the recipient.

Nonetheless, spam sent out to multiple recipients, blemishes the name of e-mail marketing (Wreden, 1999; Wright and Bolfing, 2001). Institute of Management Technology (IMT) Strategies (2001) found that the e-mails that the users never read are increasing, and the consumers tend to constraint or interrupt the e-commercial contacts. Before the universal access to the Internet was available, the e-mail spam was really a small trouble. But today, most users worldwide are confronted with this problem nearly everyday. The problem has increasingly important influence on the consuming behaviors. In an InfoWorld article (2003), a

survey disclosed that over forty percent of respondents answered unsolicited e-mail as the worst problem in the field of information technology industry in the previous year. The scale and effect of the spam prevalence implies that spam has become "significant and growing problem for users, networks and the Internet as a whole" (World Summit on the Information Society (WSIS) Declaration, 2003, paragraph 37).

Most people have some unclear awareness that spam at first came from the "spam skit by Monty Python's Flying Circus"[1] (Templeton, 2003). However, according to Templeton (2003), the history of spam can be traced back to the late 1970's with a number of network services that were sent multiple mailings, these initial group mailings were not considered annoying and as a result they got the chance of wide online spread (Templeton, 2003). Kelly (2002) explored the history of spam and believed that it was born on April 12, 1994. We can also reasonably judge that it was until the Internet was in its wide usage, when unsolicited e-mail posed a real threat.

The consensus on the definition of unsolicited e-mail is nearly reached among academia, legislature, and law enforcement, even though the actual legal practices are few. Mail Abuse Prevention System (2004) defined spam as:

"An electronic message is 'spam' if: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; and (3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender."

Although the definition of e-mail spam only denotes to the sender and recipient, they can be understood as covering individuals, organizations,

enterprises, and public institutions. It is a common concern in local, national, and international layers. During the Geneva phase of the World Summit on the Information Society, spam was identified as a potential threat to the full utilization of the Internet and e-mail (International Telecommunication Union, 2004).

Classification of spam is vital from a legal standpoint, because most spam legislation targets a particular type, such as business e-mails, or deceptive spam. The United States Federal Trade Commission identified twelve most likely spam scams: business opportunity scams, making money by sending bulk e-mailing, chain letters, work-at-home schemes, health and diet scams, easy money, get something for free, investment opportunities, cable descrambler kits, guaranteed loans or credits on easy terms, credit repair scams, and vacation prize promotions (Federal Trade Commission, 1998).

The unsolicited e-mail being a central concern, spam can also come from other sources, such as newsgroups, mobile phones Short Message Service (SMS) and instant messenger services. The legal solution to these kinds of spam is possibly in common, and countries have laws to cover spam of these and other forms of media, but this Chapter is mainly concentrated on e-mail spam.

Comparison between traditional and e-mail advertisements

Besides interpersonal interaction through e-mail, e-mail has also broad usage in advertising as well. What accompanies the unsolicited commercial e-mail is that it parallels with the legal advertisements, that is, e-mail advertisements. To better understand the phenomenon of spam

and find effective preventive mechanisms, the following section contributes to compare the advantages and disadvantages of traditional advertisements, particularly postal advertisements, and the e-mail advertisements (See Table 4).

Table 3 Comparison between traditional advertisements and e-mail advertisements

Compared Items	**Traditional advertisements**	**E-mail advertisements**
Public consciousness	Familiar	Unfamiliar
Scope	Indirectly attention-getting	Direct attention-getting
Basis of trust	Publicity	Confidentiality
Targeted audience	Mainly subscriber	Mainly non-subscriber
Censorship	Involving intermediary censorship	Lacking intermediary censorship
Costs	High	Low
Form of trade	Traditional form to traditional form	Electronic form to traditional form or electronic form
Sending and reply addresses	Provided, mostly the same	Provided or not, same or different
Receiving addresses	Limited territorial range. The wider the territorial	Unlimited territorial range. Costs independent of

	range, the higher the costs	territorial range.
Jurisdiction on disputes	Easy to ascertain according to existing laws, regulations and cases.	Difficult to ascertain. Lacking ready laws, regulations and cases.
Regulation on spam	Yes	No
Possibility of regulation on spam	Easy	Difficult
Collection of evidence on spam	Converse investigation: from consumer to registered or licensed intermediary and advertiser.	Difficult to investigate. No such registration or license.
Deterrence of punishment on spam	Strong	Weak
Possibility of recommitment of spamming	Low	High
Effect of spam	As the increase of traditional advertisements, advertisers and intermediaries better off, while recipients better off, or no change.	As the increase of unsolicited e-mail advertisements, advertisers and intermediaries better off, while recipients will worse off.

The e-mail marketing has the following advantages:

- (i) Being directly attention-getting. In most cases, the e-mail advertisements are similar to traditional advertisements in the form that the audience are not strictly divided and designated, such as the advertisements in newspapers, magazines, radios, TV programs, outdoor advertisements, or even online banner advertisement. But the e-mail marketing has the high potential to provide personalized information according to the users' different needs, hobbies, and interests. It is not strange that a professor receives advertisements on conferences, sales of books, and so on; that a professor of economics receives more specified information on conferences on economics, sales of economic books, and so forth. Many other forms of advertisements do not have so concentrated an audience. Peppers and Rogers' study (2000, p 4) discovered that the one of the success factors enabling the e-mail marketing to work well is "high response rates." The average reply rate of e-mail is 5-15 percent versus 1-2 percent for direct mail and 0.005-1 percent for banner advertising, while the e-mail marketing creates a positive effect on branding efforts (Midnet Media, 2003, p.1).
- (ii) Interactive marketing. The e-mail marketing can keep more customers. The decrease of costs and timelines permits business to communicate with customers more frequently. Regular e-mail marketing to existing customers generates a 15-50 percent increase in overall online trade. Engaging customers in a two-way dialogue enhances customer satisfaction and yield quicker response (C.f. Sandiego Media Inc., 2005).
- (iii) Confidentiality. The contents of e-mail advertisements are not necessarily confidential. E-mail is not in itself the most confidential form of communications. But for a certain users in a certain environment, the e-mail marketing is like a consult or negotiation

in a closed room. What the user decide to buy, to whom the user pays, and what and from which address the user receives, are not directly showed to anyone else. In case that the user consumes digital information, the e-mail and other electronic or online marketing might be the most suitable means.

- (iv) Low cost. The e-mail marketing lowers costs and increases profits. The e-mail marketing supplies cost-saving benefits, such as no printing, mailing or media expenditure; allows for more frequent customer conduct, which turns into higher income; average costs of 0.03 to 0.1 dollars for each e-mail, versus 2 dollars for direct post and up to 3 dollars for telemarketing; customer acquisition costs average no more than 24 dollars for e-mail versus 82 dollars for public relation, 958 dollars for print advertisements, and 1,457 dollars for radio advertisements (Midnet Media, 2003, p.1).
- (v) Diversified forms of trade. The e-mail marketing serves both traditional and digitalized goods. The goods are usually exhibited online. For traditional goods, though the electronic exhibition is not as intuitionistic as show window, or door-to-door marketing, the multimedia explanation may provide more comprehensive a presentation than any other forms of marketing. In case of digital goods, the e-mail marketing has the unique advantage in providing sample texts, and audio or video clips. In fact, many online book stores, music and video dealers, and software vendors all provide some kinds of sample to show their goods. The e-mail marketing can directly link to these online markets and goods.
- (vi) Location independent. The senders and the recipient of e-mails are both location independent. The senders can send e-mails from anywhere of the world to recipients located anywhere in the globe (if they are not outside the earth). Trans-border marketing is not

limited by the national boundary. A nearly uncontrollable route realizes the flow of goods, particularly digital goods. Even if it is traditional goods, the uncontrollable information might also cause the traditional control of trans-national flow of goods more burdensome. All in all, the trans-territorial flow of goods can benefit greatly from e-mail marketing.

- (vii) Advertisers better off; and intermediaries might also better off. As a natural effect, with the increase of e-mail marketing, the advertisers will surely better off. The voluntary intermediaries will also better off, because a portion of the profits is transferred from the advertisers to the intermediaries.

The disadvantages of e-mail advertisement are:

- (i) Most people are less familiar with e-marketing than traditional advertisements. Less people are more familiar with e-mail marketing than traditional advertising. But more and more people are more familiar with the new advertisements than ever.

- (ii) Targeting both subscriber and non-subscriber. This may induce more consumers, but may also annoy e-mail users. In fact, different forms of traditional advertisements are designed to different audience. Some forms do not distinguish subscriber or non-subscriber, such as radio, TV and outdoor advertising. But traditional postal marketing mainly targets subscribers, together with newspaper and magazine advertising. With e-mail advertisements, the businesses can limit marketing to subscribers, but can also extend to non-subscribers in order to get more profits. This advantage for senders becomes the greatest disadvantage for recipients.

- (iii) Lacking intermediary censorship. Unlike traditional advertisements that have been published on media that are managed by intermediaries, the e-mail marketing is actually direct marketing- more direct in the sense of business-to-consumer, but at the same time more indirect in the sense of no longer face-to-face. The necessary censorship on the process of information provision is missing. Subsequently, the transaction process is also less monitorable and less controllable.
- (iv) Sender's genuine identity and displayed information might be different. The falsification of sender's identity and address might mislead the consumer to open the unsolicited e-mail. The reply address might be invalid when the recipient replies to refuse further messages. The recipients have less choice in deciding whether or not to receive this kind of e-mail.
- (v) Lack of dispute solution mechanism. The possibility of regulation on e-mail marketing is law. The jurisdiction over disputes is difficult to determine. The laws, regulations, and rules, particularly international harmonization are not ready. In addition, collection of evidences is confronted with great obstacles.
- (vi) Weak deterrence of punishment on abuse of e-mail marketing. The spammers have high possibility of recommitment, motivated by monetary interests. As a result, the recipient might worse off due to absence of self-determination, while the intermediaries might also worse off due to the absence of profit transfer agreement.

The advantages and disadvantages seem more and more beneficial to the senders but less and less beneficial to the recipients. As a result, the senders have the stronger incentive to send more marketing e-mails, while

the recipients have the stronger to receive less. The overuse of e-mail marketing by the businesses will lead to underuse by the consumers.

Challenges of spam to the society

The advantages of e-mail marketing greatly upgrade the utility of e-mail in business. Both the legal and illegal commerce discover this efficient instrument in harvesting money from the market. The following summarizes a list of common challenges of legal sense that the spam brings to the society.

The first challenge is against e-mail recipients' property rights. The spammer infringes the property rights through two ways. On the one hand, spammers usually transfer the cost of sending bulk e-mails to others, including individuals, e-mail service providers (ESPs) or Internet service providers (ISPs), for example, intrusion others' computers or servers to send e-mails, or evasion the reasonable fees payable to the service providers. On the other hand, spammers usually practice fraud and deception in spamming. Spammers disguise the origin of their messages so as to ensure that the users read their messages. Federal Trade Commission (2003) reported that 66 percent of spam messages are fraudulent in the "from" or "subject" lines, or in the message itself. For example, if the subject line includes the term such as "reply", "your required information", "your free laptop", "free travel chances", etc, it is highly possibly that the users will open the e-mail and find if these are valuable messages. As for the contents, many unsolicited e-mails offer various deceptive or misleading representations. The most common fraud schemes include the Nigerian scam, online chances of making money, and

drugs sales, etc. In a successful detected case, the FBI in the United States and the Spanish police arrested 310 people who were the Nigerian conspirators of a bogus lottery scam involving 100 million Euros. The scam victimized more than 20,000 people in 45 countries (Libbenga, 2005).

The second challenge is targeted at fair trade. Contents of most unsolicited e-mails involve false advertisements or situation leading to misunderstanding. Due to the facility of transfer, such e-mails incorrectly relay erroneous information, and mislead the recipients and consumers in the bargaining. Besides the breach of the regulations on consumer protection and constitution of criminal fraud, the false advertisements might distort the normal market of goods and services, harm the normal trade order, and reduce the consumers' confidence (Taiwan Ministry of Transportation and Communications, pp. 6-7).

The third challenge is offending public morals. Unsolicited e-mails are usually not targeting specific e-mail users, among which children are highly possibly to be harassed. Because the spam messages often contain contents inappropriate for children, such as the hyperlinks of pornographic websites, pornographic pictures, and adult entertainment products and services, the pornographic spam has become a public risk for the growth of the children. From the pornography industry revenue statistics, it is apparent that the Internet-related revenue has already reached a noteworthy scale. What is worse is that the average age of first Internet exposure to pornography is as low as 11 years old, and 90 percent of the children between 8-16 years old have viewed pornography online (TopTenReview, 2005).

A relevant problem is that in some East Asian and Middle East countries, creating, copying, selling, and spreading pornography might lead to arrest and conviction (See example, Penal Law of China 1997, Articles 363-367). In addition, merely possession, and browse of

pornography is traditionally prohibited. The unsolicited e-mails make it difficult to judge whether the existing punishments are applicable to e-mail users who passively receive and "keep" e-mails with pornographic contents. For example, Management Regulations on Internet Online Service Business Location provides that the manager of Internet online service business location and the Internet users must not create, download, copy, view, release, spread or use by other means the information containing obscenity contents (China State Council Management Regulations on Internet Online Service Business Location 2002, Article 14).

The fourth challenge is a threat to cybersecurity. The security problems brought about by the spam generally require the interaction between the users and the messages. The large volume of spam, the malicious programs and malicious linkages contained in the messages are the main threats (PC World, 2003). In recent years, many of the most harmful malicious programs have been spread through exploiting e-mails.

The fifth challenge involves personal data protection. There is little exception in the available literature and legislation on spam that does not emphasize the identity theft. Many spammers send their messages by unauthorized use of other individuals or organizations' accounts (OECD, 2004). The e-mail addresses harvesting software can collect this information automatically from the webpages (Boldt, Carlsson and Jacobsson, 2004, p. 8). Therefore, the misuse of spamware and the collection and use of e-mail addresses are among the focuses of the legal regulation. If the e-mail address includes enough information to identify the user, the collection and use of such an e-mail address should under the consent of the user. Without such consent, the collection and use of the address in the spamming invalidate the privacy protection.

The sixth challenge is comprehensive. Besides the above aspects, spam is also involve in other content-related and goods-related transgresses and offences. The examples of the former category are online piracy of intellectual property, spreading of malicious programs and codes, defamation, slander, and libel, and so on. The examples of the latter category are sales of controlled goods, such as drugs, prescribed medicine, and weapons; providing services, such as auction, financing, tourism, dating, prostitution, gaming, gambling, raffling, bonus, and lottery.

In sum, at least at present, the ease of using spam to offer goods and services increases the volume of spam. Sophos statistics showed that global spam at the end of 2004 has reached 3 trillion messages, with an estimated cost of 131 billion dollars (EquIP Technology and Cipher Trust, 2004). In addition, according to an Industrial Development Corporation (IDC) study, worldwide revenue for anti-spam solutions will exceed 1.7 billion dollars in 2008 (IDC, 2005).

Costs and benefits of the spammer and the spammed

1. The costs and benefits of the sender

Whether the spammer send the spam is thought by economists as controlled by "the invisible hand"[2] of interests. According to Khong (2004), although it is difficult to measure the costs and benefits of the spammer, if the benefit obtained from the activity outweighs the cost, then the spammer will undertake the spamming activity. It follows that if there is one successful commercial transaction, the spammer can realize his/her

benefit. The costs that are involved in the spamming can be roughly estimated in the following aspects:

First, bandwidth cost. It is inevitably to involve the cost of bandwidth in the message sending. According to Living Internet (2005), as a form of communication across global distances, e-mail is relatively the cheaper way. Based on a very conservative cost of 10 dollars a gigabyte for bandwidth, Living Internet showed that every 50 thousand e-mails cost one dollar in bandwidth costs. That is to say, the per message bandwidth cost is only 0.000020 dollars. If the spammers undertake these costs, the monetary investment will be very tiny compared with the possible income from the spamming.

Second, costs in sending message. Besides bandwidth costs, there are also other costs associated with sending a message. This is usually measured by how much the spammer is willing to do the spamming. According to Goodman and Rounthwaite (2004), the higher price is about 0.001 dollars per message, the lower price is about 0.000025 dollars per message. The cheaper charges range from 0.0001 to 0.0003 dollars per message.

Third, to obtain users' e-mail address may also involve some kinds of costs. But the actual cost may depend on the ways in which the addresses are harvested. According to Sadowsky, the spammer can obtain users' e-mail address in the 13 situations (Sadowsky et al., 2003, p. 55). But obviously, the most convenient and least expensive way is to harvest e-mail addresses automatically with specific software. The software are also available from Internet, either free of charge or with an inexpensive price.

Even trickier, the revenue of spammer from sending message has been found high in a few studies. Goodman and Rounthwaite (2004) cited the following information in clarifying how much per message revenue

would be. They cited that Grimes (2003) had reported one person had had the revenue of as much as 0.0005 dollars per message, but was willing to do as little as 1,000 dollars per mailing: as little as 0.0000125 dollars per message. Other information they cited was from a *Wall Street Journal* article, reporting that a person obtained 360 dollars or sending 10 million messages, around 0.000036 dollars per message (Moran, 2002).

The above information indicates that the costs of the spammer are increasingly low, while the revenue is increasingly high. Hansell (2003) found that compared to the cost of 190,000 dollars for one million conventional bulk-rate postal mails, the marginal cost of sending a marketing message to one million recipients by electronic mail is less than 2,000 dollars. He estimated that commercial e-mail is profitable if one recipient in 100,000 makes a purchase. The fact that the spam can be sent at very low cost and in a great quantity has attracted direct marketing companies to use spam e-mails for advertisement. Cobb (2003, p.2) suggested the concept of "the parasitic economics of spam," meaning that the act of sending a message costs the sender less than it costs all other parties impacted by the sending of the message. In reality, some spammers pay nothing for sending their messages, hijacking resources that belong to others.

2. The costs and benefits of the spammed

The costs induced by the spam to the spammed have a wide coverage. They include the waste of the users' time, bandwidth and storage, cost of anti-spam solution, and cost of overloading at the mailbox.

First, the topic of whether the waste of time in dealing with the spam is disputable. Spam messages are annoying in that the users have to

spend time and money dealing with them. In daily life, some people argue that they know e-mail well and it is easy to identify spam messages from useful e-mails. Even if there are some bulk mails, the user needs only a few seconds to browse the address, subject, content, signature, etc in making a judgment. To delete them is also not so complicated. They doubt how the problem can be so serious and so wasteful. In fact, meeting with messages well falsified in address and subject lines, the user is impossible to judgment whether this is a spam or a message from a contact. When the message is open, the user has to browse the contents and signature to make the final decision. If the message begins with information of his interests, the users have to spend yet more time to decide whether or not to delete the message. The average time and money lost in processing a single message might not be so significant. But the aggregate loss of time and money in aggregate taken in dealing with these messages might be huge.

The time the users spend on dealing with spam messages can be quantified in a way of counting numbers of messages the users receive everyday, and the time spent on making judgment on whether the messages are spam and deleting them. In some services companies, the treatment of these messages needs special care so as not to ignore the customers' requests, complaints, and business communications. EquIP Technology and Cipher Trust (2004, p.1) found that the average e-mail user receives up to 70 e-mails a day. According to Zeller (2005), a December 2004 survey suggested that Internet users spend an average of 10 working days per year dealing with spam, and at least some industry analysts estimated that the yearly cost of spam to business due to lost productivity and additional network maintenance costs will be around 50 billion dollars.

Second, spam also induces costs of the bandwidth and storage. Khong (2001) pointed out that in addition to the losses of the users, the spam also has great impact on e-mail service providers (ESPs). The European Union estimated the global bandwidth costs of spam at 8-10 billion dollars annually (EquIP Technology and Cipher Trust, 2004, p. 2). The potential threats might even severe to cause an ESP's network to shut down (Goodman, 2000). The interruption of services is unfortunate for both the providers and users in causing business, confidence, and other losses.

Third, the influx of spam has caused many people and organizations to deploy some form of anti-spam solution. A European Commission study estimated that the costs associated with these solutions might come up to 10 billion euros per year worldwide (Gauthronet & Drouard, 2001). Gartner Consulting (1999, p. 4) found that the longer an e-mail user kept an e-mail account, the more likely he would be spammed. It indicates that spam is a more severe threat to the established users than the new comers, and a more severe threat to the users more dependent than the users less dependent on e-mail. That is to say, the more possible the users benefit from the e-mails, the more possible they bear losses from spam. The increased profits of the spammer are just based on the increased loss of the spammed. It is reasonable to deduce that the spamming business would growth in pace with the development of the e-commerce.

Finally, another side effect of the spam is that it corrupts e-mail services, fills up users' mailbox with useless information, and decreases the usefulness of the e-mail service. Even worse, if the e-mail address has ever been put on the institution's website, or personal homepage, it is highly possibly that the address will be harvested, sold, and abused by spammers. Under these circumstances, the number of spam messages might increase in an unexpected pace. I keep an e-mail address provided by a high profile website. It has been put to the Internet for a few

occasions. Recently, the average number of spam messages per day may reach one hundred. Although the fortunate bulk mail prevention function by the provider works well, and most bulk mails are automatically put into the specific folder, sometimes, it is inevitable that useful messages are also identified as spam, and the inbox is still filled with dozens of spam messages everyday. Most of the spam messages can really be judged through the subject or address lines. To delete them needs a few seconds everyday. The most annoying is that it is really difficult to look for the useful messages from dozens of useless messages received unexpected. The final solution is to notice the contacts the change of the address.

In fact, from the analysis above, we can identify nothing useful and beneficial to the spammed. They undertake pure losses, not only the monetary, but also the psychological.

The limitation of technological and market solutions

The technical solutions to spam involve complicated mechanisms, which are not the primary concern of this Chapter. But the main means are filtration and blacklist. The former is used to filter the sources, headers, and content. The latter is used to mark the refused IP addresses. Practices proved that the technical filtration often misjudges, deletes, and blocks the useful and legal e-mails, and incapable to effectively stop sending of spam from the sources. At the same time, the technical solution also has influences on the transmission of the e-mail service providers and the terminals (Taiwan Ministry of Transportation and Communications, p. 13). It is also possible that the recipient install filtering software to prevent spam. But it is still less effective.

In the meanwhile, spam technology and anti-spam technology are competing in contesting with the market. The technical capacity of tracing spam source is always limited (Taiwan Ministry of Transportation and Communications, p. 14). Besides the economic incentive in spamming and the technical limitation in anti-spamming, the issue is worsened by the extra costs of the service providers on improving computing ability to filter the spam, and the potential risks of misjudgment and breach of constitution. If there is no legal warrantee and liability, the possible technical solutions might also be discarded. The technical solution could be effective only when certain legal basis is ready to divide the risks between the senders, the service providers, and the recipients.

Given the technological solution is not the unique way; the legal regulations on spam are further justified by the limitation of non-legal solutions. The following analyzes the disadvantages of the non-regulatory measures.

Theoretically, the prohibition of spam could be integrated into regulations on the protection of consumers' rights. But the traditional laws can at most extend privacy protection to the activities of misuse of mail lists according to the personal data protection law, such as in Taiwan. However, this protection is limited to eight industries and cannot provide complete protection for consumers (Taiwan Ministry of Transportation and Communications, p. 6).

Self-regulation is practiced by various coalitions of anti-unsolicited e-mails. The goal of these coalitions is focused on that the consumers enjoy the right to accept or refuse the bulk mails, and that the Internet resources and privacy should be sufficiently respected. The awareness of the consumers, website managers, and the Internet service providers helps to take coherent actions in combating spam, and enhancing the quality of Internet services.

Observing the current situation, we can find that the consumers' protection and self-regulation mechanisms are both less effective as well. On the contrary, the problem of spam is growing more serious. Therefore, clear rules are needed to define the scope of the spam and offer suitable punishment, neither throttling e-mail as an e-marketing tool nor leaving it as it is.

Legal regulations on spam

1. Basic approaches within the legal framework: opt-in vs. opt-out

In dealing with spam, various technological solutions are being created, used, and proved to be less effective. As a necessary remedy of the problem of the spam, legal framework must also be used to fight against spammers.

The first step in taking a legal action is to consider whether the consent of the address owner should be obtained prior to the sending of the spam message. If the prior consent is necessary, the method is called "opt-in". If the prior consent is not required, the method will be "opt-out".

The opt-in mode fully takes care of the free will in receiving messages. Through receiving e-mails, the recipients can acquire certain information. But the privacy of the recipients and the consumers must be taken into account. The right of privacy is now widely recognized and protected in constitutions and laws worldwide. Remedies for infringement of this right have also implemented through civil law or criminal law. Any potential threats to the privacy should be considered in advance of the activities. The opt-in mode might better serve this goal in the information

age. Opt-in mode is adopted in Australia, China, and the European Union (for example in the United Kingdom).[3]

With Directive 2002/58/EC, the European Union has adopted an "opt-in" approach for commercial communications by e-mail. The Article 13 of the Directive titled "*Unsolicited communications*" provided that:

"The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent."

However, Article 13.2 also leaves an open door for a kind of special opt-out choice:

"Where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use."

Article 13.3 explicitly limits the use of unsolicited communications for purposes other than direct marketing. They are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation. This provision ensures the effective opt-out in cases the users choose to interrupt the subscription after either opt-in or limited opt-out.

The general requirements in sending commercial e-mails are by the way of ensuring the real identity, and address. Article 13.4 of the Directive prohibits the "disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease."

The Article 13.5 of the Directive further provides that the subscriber in provision about the definition of unsolicited communications and the limited opt-out provision shall apply to natural persons. But it requires the Member States to sufficiently protect the legal interests of other subscribers.

The Directive helps to establish a legislative model within the framework of the European Union. Opt-in approach has been adopted in most EU Member States, and is under consideration in some other countries (Sipior, Ward and Bonner, 2004, p. 62). Under the opt-in approach, the burden is on the senders to offer the "opt-in" option. For the e-marketing as a whole, in the case of sending in goodwill, the user can save time and costs in processing the irrelevant messages. In the case of sending mala fide, the recipients can prevent in advance. The main advantages of opt-in e-mail services are timeliness, convenience, and control.

Compared with the opt-in mode, the opt-out mode considers the difficulty of the industry in acquiring the users' written consent. If the use of such information were prohibited, the industries of financing service, direct marketing, and customer credit would be directly impacted. The advantage of the opt-out mode than written consent is that it can balance the personal privacy and right of individual consumer, offering the opportunity for consumers to express their will on whether or not to receive specific category of e-mails. The opt-out mode is adopted in Canada, Japan, South Korea, Singapore, Taiwan, and the United States.[4]

In the North America, the United States CAN-SPAM Act superseded more than 30 state laws covering spam. The legislation adopts an opt-out approach under strict limitations. Section 5 of the Act provides the requirements for transmission of messages:

1. Prohibition of false or misleading transmission information. The Act outlaws sending commercial e-mail message, transactional or relationship message with header false or misleading information to a protected computer (Section 5 (1)). Even if the header information is "technically accurate", including the originating e-mail address, domain name, or IP address, but when they are obtained by means of false or fraudulent pretences or representations, they are regarded as "materially misleading" (Section 5 (1)(A)). If the sender "knowingly use another protected computer to relay or retransmit the message" in order to disguise the origin, the header information shall be regarded as "materially misleading" (Section 5 (1) (C)).
2. Prohibition of deceptive subject headings. The Act outlaws sending commercial message if know or should know that "a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message" (Section 5 (2)).
3. Prohibition of omitting return address or comparable mechanism (Section 5 (3)). The Act outlaws sending commercial e-mail message without displaying "a functioning return electronic mail address or other Internet-based mechanism" (Section 5 (3) (A)). The Act further requires that the return address or other mechanisms can be used by a recipient to opt-out by the way designated in the message (Section 5 (3) (A) (i)). The return address must be available for "no less than 30 days" after sending the message ((Section 5 (3) (A) (ii)).

4. Prohibition of transmission of commercial electronic mail after objection. In the case of opting out by a recipient, then sending e-mail more than 10 business days after the receipt of such request is unlawful (Section 5 (4)).
5. Inclusion of identifier, opt-out, and physical address in commercial electronic mail (Section 5 (5)).

The effective opt-out mechanism should be "sending once, and identifying once." It means that the messages are sent to the recipients only once if the recipients do not receive such messages any longer, and the recipients need to identify the same source of the same messages only once before he/she decide to refuse or subscribe it. Under such circumstances, mode of the users searching information changes to the mode of the users judging whether the coming information is valuable. Thus it is less wasteful for both the senders and recipients, if the senders are sending the information in goodwill.

The disadvantage of this approach is that it increases the costs of processing information in distinguishing those useful from useless, wasting work time, human resources, and money. For overall comparison of these two means, see Table 2 below.

Table 4 Comparisons between Opt-in and Opt-out (Hong Kong Information Security Website, 2005)

Approaches	Advantages	Disadvantages
Opt-in	Burden on senders to offer opt-in option. Recipients save time and costs in processing irrelevant messages.	Malpractice of some traders. Lead to insufficient, asymmetry information, and increase costs of information searching. Malicious senders join the mail lists, and

	Recipients prevent spam in advance.	send more specialized spams.
Opt-out	Burden on recipients to inform opt-out. Sending once, identifying once. Information searching changes to information selecting.	Opt-out becomes confirmation to spammer. Cost of processing information increases.

The distinction between opt-in and opt-out modes is easy to make. But in the case of opt-out mode, there exist a special case that needs a special legal answer. If the recipient of the opt-out e-mail sends back the message with selected items that he consents to receive or refuses to receive further e-mails, it is purely the purpose of opt-out. The recipient bears the expenses involved in the process. But if the recipient does not reply to the opt-out offer, the judgment of whether the recipient is willing to receive further e-mail cannot be made without an explicit legal provision. The law must give an indubitable answer.

2. Regulated scope of unsolicited message

The contents and categories of regulated unsolicited message vary among countries from each other. In the aspect of the contents of the regulated unsolicited message, countries generally target at commercial communications, such as in Australia, Japan, Korea, the United Kingdom, and the United States. The Australia Act on Unsolicited Electronic Information 2003 applies to "commercial electronic message," unless it is exempted. The Korea Act on Promotion of Information and

Communication and Communications Network Utilization and Information Protection of 2001 defines unsolicited messages to advertisement information for the purpose of earning profit or commercial advertisement. The United Kingdom Privacy and Electronic Communications (EC Directive) Regulations 2003 applies to e-mail sent for the purpose of direct marketing. The United States CAN-SPAM Act defines "commercial electronic message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." (Section 3 (2)) Hong Kong Bill against Unsolicited Electronic Message 2005 proposes regulation on unsolicited commercial electronic message. Non-commercial message, such as the communications of governments and citizens, contribution appeal of the charity or religious organizations, communications of political parties are not limited. The provision of China Management Measures on Internet E-mail Services 2005 is wide enough to cover all kinds of e-mail messages.

In the aspect of the forms of the regulated unsolicited messages, there are also different legislations. The law in the United States limits the message to commercial e-mail. Similarly, China also limits the form of spam to e-mail. The mobile message is excluded.

Other countries adopted broad legislation to outlaw more kinds of messages. The regulated electronic message in Australia covers e-mail, instant message, and telephone. The scope of the United Kingdom law covers automatic calling system, facsimile, and e-mail. The Section 5 of Australia Spam Act 2003 defines the purpose of the Act to regulate commercial electronic message including e-mail, instant message, telephone, and similar messages. But voice calls are excluded: If a message is sent by way of a voice call made using a standard telephone

service, the message is not an electronic message. Korea outlaws unsolicited e-mail, telephone, facsimile, or other media prescribed by the Presidential Decree. The term "other media" is obviously used to cover short message service (SMS) and other electronic communications services. At the same time, Korea also specifies those messages sent to recipients in violation of law as spam (Personal Data Dispute Mediation Committee, Korea Information Security Agency, 2003, p. 5-6). The Hong Kong bill covers all the unsolicited commercial electronic messages: e-mail, facsimile, instant message, and multimedia message, messages generated automatically by devices, including audio or video messages recorded beforehand and sent through the Interactive Voice Response System (IVRS) (Xie, 2005).

3. Labeling of commercial e-mail

Labeling consists of displaying standard identifying labels in the subject line or header. Some countries require senders to label certain kinds of messages, but others do not require it (Ahn, 2004). In order to make it possible for the e-mail service providers and the recipients to distinguish and filter the e-mails before open them, the general provision requires the sender add some words in the commercial e-mails, such as "advertisement." China requires labeling of "Advertisement" in Chinese or "AD" in English. Taiwan Draft Regulations on Unsolicited Commercial E-mail requires labeling of "Commercial," "Advertisement" in Chinese or "ADV" in English. The bill also authorizes the agency in charge of the regulation to publish other labels that can be used to identify the commercial e-mail. In Korea, Article 11 of the Ordinance of the Ministry of Information and Communication of the Act (Act on Promotion of

Information and Communication and Communications Network Utilization and Information Protection of 2001) requires an "ADV" label. But in order to prohibit the irregular forms of labels such as "A*D*V" and "A~D~V", the Ordinance was revised in 2002 to exclude the irregular forms. The revision also requires an "ADLT" (adult) label if the e-mails are for adults. In June 2003, the Korea law further requires to "include the '@' (at) symbol in the title portion (right side) of any commercial e-mail address, in addition to the words 'Advertisement' or 'Adult Advertisement' as applicable." (Korea Information Security Agency, 2003).

Many states in the United States require a label in the subject line of an e-mail that will alert recipients that the message is an advertisement. This includes two modes: unsolicited sexually explicit messages must contain a label of "ADV: ADULT", "ADV: ADLT", "ADULT ADVERTISEMENT", "ADV: ADULT ADVERTISEMENT" at the beginning of the subject line; unsolicited commercial e-mail messages must contain a label of "ADV:" or "ADVERTISEMENT". False, deceptive, or misleading subject lines are outlawed. Table 3 shows the different legislation modes on the problem of labeling in the United States (for a complete summary of the U.S. state laws, see Sorkin, 2006).

Table 5 Legislation Modes concerning Labeling

Legislation Modes	**Categories**	**Label**	**States**
Requirements of Label	Unsolicited sexually explicit messages	"ADV: ADULT", "ADV: ADLT", "ADULT ADVERTISEMENT", "ADV: ADULT ADVERTISEMENT"	Alaska, Arkansas, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Missouri, New

			Mexico, North Dakota, Oklahoma, Pennsylvania, South Dakota, Tennessee, Texas, Utah, and Wisconsin
	Unsolicited commercial e-mail messages	"ADV:" or "ADVERTISEMENT"	Arizona, Colorado, Michigan, and Nevada
Prohibition of False, Deceptive, or Misleading Subject Lines			Arizona, Illinois, Indiana, Kansas, Maryland, Minnesota, Missouri, North Dakota, Oklahoma, Pennsylvania, South Dakota, Texas, Washington, West Virginia, and Wyoming

In order to avoid possible disputes and damages in the direct marketing through e-mail, effective tracing of senders is critical. Laws require the sender to provide correct header of the e-mail. The Section 5 (a) (1) of United States CAN-SPAM Act, Article 3 (3) and Article 5 of Japan Specified Commercial Transactions Law for Appropriate Transmission of Specified E-mails 2002 all provide the similar requirement. The sender's identity information is also an important

requirement in commercial e-mails. The Section 5 (a) (5) of the US Act, and Article 3 (2) of the Japan Law both make such provisions.

In the United States, states have taken different steps to criminalize the act of sending unsolicited commercial e-mail containing false, falsified or missing routing information, or misrepresent or obscure the point of origin or routing information; the sale, distribution, and possession with intent to sell software that is designed to falsify routing information; and unsolicited commercial e-mail using a third party's Internet address or domain name without permission. Some states require that the unsolicited commercial e-mail must include the sender's name, street address, and e-mail address, along with opt-out instructions (Coalition Against Unsolicited Commercial Email, 1999). The following Table 4 compares the differences between the legislation modes of the U. S. states.

Table 6 Legislation Modes concerning Identity

Criminalization or Requirements		**States**
Criminalization	The act of sending unsolicited bulk e-mail containing false, falsified or missing routing information, or misrepresent or obscure the point of origin or routing information	Arizona, Arkansas, Colorado, Connecticut, Delaware, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, and Wyoming
	The sale, distribution,	Arkansas, Connecticut,

	and possession with intent to sell software that is designed to falsify routing information	Delaware, Illinois, Kansas, Louisiana, Michigan, Nevada, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Virginia, and West Virginia
	Unsolicited commercial e-mail using a third party's Internet address or domain name without permission	Arizona, Arkansas, Colorado, Idaho, Illinois, Indiana, Iowa, Kansas, Maine, Maryland, Minnesota, North Dakota, Oklahoma, Pennsylvania, Rhode Island, Texas, Washington, West Virginia, and Wyoming
Requirements	Require that the unsolicited commercial e-mail must include the sender's name, street address, and e-mail address, along with opt-out instructions	Arkansas, Colorado, Indiana, Iowa, Kansas, Maine, Minnesota, Missouri, Nevada, new Mexico, Ohio, Oklahoma, Rhode Island, Tennessee, and Utah

These different provisions within one nation indicate that the law enforcement is confronted with either the jurisdictional gap or overlap, besides possible consistency and coordination.

4. Criminal liability, administrative liability, civil liability, and international cooperation

The prohibition of spam is ensured by liability mechanisms. The liabilities for spam can take the forms of criminal, administrative and civil liabilities. In nature, the criminal liability is the most severe and deterrent one. The administrative and civil liabilities are less deterrent. But deterrence is not the only factor in determining the adoption of liabilities. The most deterrent liability might also be the most costly and thus less efficient in economic sense. Therefore, other liabilities can have comparative advantages. In either case, the international coordination and cooperation are necessary.

In some of the U.S. states, spam has been criminalized by state laws, such as Colorado, Nevada, Pennsylvania, Connecticut, Delaware, Louisiana, North Carolina, and Virginia. In some other jurisdictions without statutes regulating commercial spam, unsolicited e-mail is usually regulated with reference to harassment, stalking, and sexually explicit communication to minors, such as in Hawaii, Wisconsin, and Maryland (Gilbert & Harrison-Watkins, 2001). The Section 4 of 2004 CAN-SPAM Act prohibits using a computer without authorization to send commercial e-mail; falsifying header information in sending commercial e-mail; and registering e-mail accounts with false identifying information, and using those accounts to send commercial e-mail. Under the Act, violations of the provisions above can result in fines and imprisonment of between one and five years depending on the seriousness of the violation and other factors.

In exploring the criminal liability for spam, there are some issues deserving reconsideration.

Firstly, although the overall losses caused by spam are huge, the average loss of a single user by a single message might be very tiny. Every single user might lack the incentive to report and provide evidences to the law enforcement. If they do so, the process might involve more expenses of time, money, and energy than merely being spammed, without any

expected reward. A simple reaction of users against spam might be to ignore it, until they have more sufficient psychological pulse and economic motive to report it.

Secondly, the cost of tracking down spammer is high (Prince, 2004). Although there are cases of harsh criminal sanctions, such as that a Virginian spammer was sentenced to nine years in prison for sending 10 million e-mails each day (Wakefield, 2005), the cases of large damages, such as that another spammer was sued by AOL for 7 million dollars (Ibid), and that a Florida-based spammer, James McCalla was imposed the uncollectible fine of 11 billion dollars for sending over 280 million unsolicited e-mail messages, and an enforceable mechanism of banning him to use the Internet for three years (Arnfield, 2006). Spamhaus estimated that spam would account for 95 percent of all e-mails by mid-2006 (Wakefield, 2004).

Thirdly, the countries adopted different legal approaches, such as opt-in, opt-out, and even no regulation at all. Within each mode, the nature and scope of the regulated messages varies from one country to another. The countries without anti-spam law neither protect the spammed nor prevent the spammer. The users become the potential targets of the spam, while the spammers might emerge in these countries or move to these countries to spam. Every country has the possibility of becoming a safe haven for spammers. This makes it less effective to coordinate internationally.

Fourthly, in addition to the high cost, and the legal and jurisdictional differences, the uncontrollability of the e-mail communications, and the trans-territorial or trans-national distribution of both the spammers and the spammed determine the very low detection and conviction probability. The traditional view supposed a more severe penalty as a more suitable deterrence. But if the probability is near zero, even the highest

punishment does not work. All these factors have influence on the effectiveness of criminal liability.

In China, the regulation and punishment of spam are realized through administrative liability. The Article 24 of the Law provides that sending unsolicited e-mail, sending e-mail with false header and labeling, or sending e-mail to recipient who opt-in previously but opt-out subsequently, should be corrected under the order of Ministry of Information Industry or Bureau of Communications Management, and imposed a fine no more than 10,000 RBM Yuan (about 1,000 euros); those who obtained illegal income, should be imposed a fine no more than 30,000 RMB Yuan (about 3,000 euros).

It is also possible to take civil actions against spam senders. First of all, because the ISPs' systems are repeatedly burdened by huge volume mailings, they can incur noteworthy cost. Thus, they have the choice of seeking financial compensation through civil action. Generally, civil laws that apply to damages resulting from wrongful actions or breaches of contract would apply to conventional and online activities equally (Ferguson & Piragoff, 1997).

Another form of civil action can also protect recipients from spamming. Damages are a favorable deterrent against spam. Laws in some of the U.S. states provide statutory damages to individuals and ESPs. These damages vary from 10 dollars per message in Colorado and Iowa to 500 dollars in Rhode Island.

Law enforcement needs the harmonized international actions. There have been a number of international initiatives to deal with the problem of trans-border scams. The Organization for Economic Cooperation and Development adopted new guidelines in June 2003 to promote international cooperation against trans-border fraud and deception.

Recent trends in international cooperation have been between industries, organizations and the consumer or citizen, and between industries and government (Ahn, 2004). Important multi-lateral organizations include the Organization for Economic Cooperation and Development, International Telecommunication Union (ITU), APEC, Internet Corporation for Assigned Names and Numbers (ICANN) and International Consumer Protection and Enforcement Network (ICPEN). In order for the international cooperation to be timely and effective, it should include various different communities (OECD, 2004). In dealing with the problem of spam, the new-styled international cooperation is an urgent call. As of 2005, International Council on Internet Communications was formed to coordinate international efforts to stop spammers (News Target, 2005). Given spam is still in its rapid developing stage, we cannot expect any of such institutions are able to solve the problem in a predictable period.

International action might meet obstacles impossible to overcome. The senders and recipients in opt-in countries and the opt-out countries might first meet with unsolvable vicious cycle. The users of opt-in countries might always feel that they are annoyed by the senders of the opt-out countries. The users of the opt-out countries might feel that they are less informed by the businesses of the opt-in countries. The businesses of the opt-out countries might also feel that they are guilty of spamming users of opt-in countries. The senders of the opt-in countries might feel that they are less competitive in the e-marketing in the global market, and so forth.

Furthermore, we mentioned the different provisions of the subject line. The English-speaking countries will surely require a label in English, such as "ADV", and so forth. Other countries require a label either in their native languages or in English. This brings about little problem within one jurisdiction. The problem is that e-mail advertisements are neither

language dependent nor jurisdiction dependent; laws of most countries are, nevertheless, jurisdiction dependent, protecting recipients and preventing senders in one jurisdiction. Neither are the spammers from abroad are well punished, nor are the spammed from abroad well protected. Trans-national spamming is a problem that domestic laws are reluctant to deal with.

Finally, it is less possible to determine whether a message with a specific label is spam according to the domestic laws. If a Chinese sender, fully coincident with Chinese law, sends a message with a label in Chinese character to a user in Japan, who is also a Chinese citizen, he/she might identify this Chinese message as spam according to Japanese law, whether he/she consent to receive such a message or not. Because he/she receives the message in Japan, where only Japanese law applies, he/she can take an action against this Chinese sender on the basis that this message provided the irregular label.

From the above analysis, international cooperation should not only propel unified rules, but also hold spammers liable for trans-border spamming. More than ever, an international anti-spam agreement is necessary.

Conclusion

Spammers are motivated by greater benefits from spamming than other kind of direct mailing. The growth of spam despite the increase of efforts suggests that any previous solution cannot work alone. Comprehensive mechanisms must be established to protect the spammed and to discourage the spammer. To balance the liability among the spammer, the

spammed, and the intermediaries, criminal sanctions, civil remedies, and international harmonization are all constituents of the effective legal framework.

References

1. Ahn, S. (2004, January 22). Background Paper for the OECD Workshop on Spam, OECD Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy.
2. Arnfield, R. (2006, January 5). Florida Slaps Spammer with $11 Billion Fine. Retrieved March 15, 2006 from http://www.seeweekly.com/hosting-florida-slaps-spammer-with-11-billion-53252.html
3. Boldt, M., Carlsson, B., & Jacobsson, A. (2004). Exploring Spyware Effects. Retrieved March 15, 2006, from http://psi.bth.se/mbo/exploring_spyware_effects-nordsec2004.pdf
4. Coalition against Unsolicited Commercial Email (1999, December). *CAUCE News*, 3 (4). Retrieved March 15, 2006, from http://www.cauce.org/node/110
5. Cobb, S. (2003). The Economics of Spam. Retrieved March 15, 2006, from http://www.spamhelp.org/articles/economics_of_spam.pdf
6. Direct Marketing Association. Executive Summary of International Spam Laws. (n.d.). Retrieved March 15, 2006, from http://www.the-dma.org/antispam/spamlaws.html

7. EquIP Technology & CipherTrust. (2004). Spam and Productivity Theft- a Growing Concern for UK PLC. Retrieved March 15, 2006, from http://www.apig.org.uk/equipandciphertrustevidence.doc
8. Federal Trade Commission (1998, July). FTC Names Its Dirty Dozens: 12 Scams Most Likely to Arrive via Bulk E-mail, FTC Consumer Alert.
9. Federal Trade Commission. (2003, June 15). *National Do-Not-E-mail Report to Congress*, Author.
10. Ferguson, P., & Piragoff, D. K. (1997). Internet and Bulk Unsolicited Electronic Mail. Retrieved March 15, 2006, from http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwapj/SPAM_1997En.pdf/$FILE/SPAM_1997En.pdf
11. Gartner Consulting. (1999). ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition, Author.
12. Gauthronet, S., & Drouard, E. (2001). *Unsolicited Commercial Communications and Data Protection*. Brussels: Commission of the European Communities, Internal Market Directorate General.
13. Gilber, S. & Harrison-Watkins, T. (2001). SPAM: Survey of State and Federal Legislation. Retrieved March 15, 2006, from http://gsulaw.gsu.edu/lawand/papers/su01/gilbert_harrison/
14. Goodman, J. T., and Rounthwaite, R. (2004). Stopping Outgoing Spam. In: *Proceedings of the 5th ACM Conference on Electronic Commerce*, 17-24 May, ACM Press, pp. 30-39.
15. Goodman, P. S. (2000, December 13). Verizon Online User's E-mail Problems Persist, *Washington Post*, E01.
16. Grimes, A. (2003, May 22). Digits: Spam Pays. *The Wall Street Journal*, B3.

17. Hansell, S. (2003, July 29). The High, Really High or Incredibly High Cost of Spam. *The New York Times*.

18. Hong Kong Information Security Website. (2005, July). Approaches to Cope with Unsolicited Messages. Retrieved March 15, 2006, from http://www.infosec.gov.hk/english/antispam/e-mail/e-mail6.htm

19. IDC (2005, February 24). Worldwide Revenue for Antispam Solutions To Reach Over $1.7 Billion in 2008, IDC Reveals. *IDC - Press Release*. Retrieved March 15, 2006, from http://www.idc.com/getdoc.jsp?containerId=prUS00085505

20. IMT Strategies. (2001). Raising the Stakes in Permission Marketing. Stanford: Author. Retrieved March 15, 2006, from http://www.imtstrategies.com/download/TI13.01.pdf

21. InfoWorld (2003, July). What is the Worst IT Disaster of the Last Year. *InfoWorld*.

22. International Telecommunication Union (2004). *Meeting Announcement: ITU WSIS Thematic Meeting on Countering Spam*. Geneva: CICG, July 7-9.

23. Kelly, J. S. (2002). A Brief History of Spam. Retrieved March 15, 2006, from http://www-106.ibm.com/developerworks/linux/library/l-spam/l-spam.html

24. Khong, W. K (2001, October). The Law and Economics of Junk E-mails (Spam). Retrieved March 15, 2006, from http://www.frg.eur.nl/rile/emle/Theses/Khong.pdf

25. Khong, W. K. (2004). An Economic Analysis of Spam Law. *Erasmus Law and Economics Review*, 1 (February), 23-45.

26. Korea Information Security Agency (2003). Korea Spam Response Center-Legislation for Anti-Spam Regulations: Mandatory

Indication of Advertisement. Retrieved March 15, 2006, from http://www.spamcop.or.kr/eng/m_2.html

27. Korea Information Security Agency, Personal Data Dispute Mediation Committee (2003). *Introduction to Act Related to Spam in Korea*, Author.

28. Libbenga, J. (2005, July 21). Biggest 419 Bust in History. Retrieved March 15, 2006, from http://www.theregister.co.uk/2005/07/21/scammers_nabbed/

29. Living Internet (2005, June 6). E-mail Spam. Retrieved March 15, 2006, from http://www.livinginternet.com/e/et_spam.htm

30. Mail Abuse Prevention System (2004). Definition of Spam. Retrieved March 15, 2006, from http://www.mail-abuse.comSpam-def.html

31. Midnet Media (2003). Economics of E-mail. Retrieved March 15, 2006, from http://www.midnetmedia.com/BUILD/PDF/MMPG4.pdf

32. Moran, J. M. (2002, June 30). Spam King Living High in the Bayou. *The Hartford Courant*.

33. News Target (2005, April 28). New International Anti-Spam Council Pledges to Fight Spam around the World. Retrieved March 15, 2006, from http://www.wired.com/news/technology/0,1282,64383,00.html?tw=wn_tophead_5

34. Niall, J. (2000). *The E-mail Marketing Dialogue*. Cambridge: Forrester.

35. OECD (2003). *OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders*, Author.

36. OECD (2004). *Second OECD Workshop on Spam: Report of the Workshop*, Author.

37. PC World (2003, August 29). Sobig May Be Working for Spammers. Retrieved March 15, 2006 from http://www.pcworld.com/news/article/0,aid,112261,00.asp

38. Peppers, D. & Rogers, M. (2000). *E-mail Marketing Maximized* . Stanford: Peppers.

39. Prince, M. (2004). How to Craft an Effective Anti-Spam Law. June. Retrieved March 15, 2006, from http://www.itu.int/osg/spu/spam/

40. Radical Group (2005). *The Radical Group, Inc. Release Q1 2005 Market Numbers Update*, Author.

41. Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B. J., and Schwartz, A. (2003). *Information Technology Security Handbook*. The International Bank for Reconstruction and Development.

42. Sandiego Media (2005). E-mail Marketing Solution. Retrieved March 15, 2006, from http://www.sandiegomedia.com/cgi-bin/main/co_disp/displ/strfnbr/101/pgname/e-mail_marketing_benefits

43. Simon, H. A. (1982). *Designing Organizations for an Information-Rich World: Models of Bounded Rationality*. MIT Press.

44. Sipior, J. C., Ward, B. T., & Bonner, P. G. (2004, June). Should Spam Be on the Menu? *Communications of the ACM*, 47 (6), 59-63.

45. Sorkin, D.E. (2006). Spam Laws. Rretrieved March 15, 2006, from http://www.spamlaws.com

46. Taiwan Ministry of Transportation and Communications, The Directorate General of Telecommunications (2005). Questions and Answers on Relevant Topics about Draft Regulations on Unsolicited

Commercial E-mail. Retrieved March 15, 2006, from http://www.dgt.gov.tw/chinese/ncc/mail-requlation/ncc-SPAM-Q&A-940215.doc

47. TopTenReview (2005). What Makes a Great Internet Filter Software Solution? Retrieved March 15, 2006 from http://internet-filter-review.toptenreviews.com

48. Templeton (2003). Origin of the Term "Spam" to Mean Net Abuse. Retrieved March 15, 2006, from http://www.templetons.com/brad/spamterm.html

49. Wakefield, J. (2005, April 21). UK Laws Are Failing to Deter Spam. *BBC News*. Retrieved March 15, 2006, from http://news.bbc.co.uk/1/hi/technology/4466053.stm

50. World Summit of Information Society (2003). *Declaration of Principles-Building the Information Society: A Global Challenge in the New Millennium*, Author.

51. Wreden, N. (1999, January 9), Mapping the Frontiers on E-mail Marketing. *Harvard Management Communication Letter*, 6-8.

52. Wright, N. D., & Bolfing, C. P. (2001). *Marketing via E-mail: Maximizing its Effectiveness without Resorting to Spam*. James Madison University.

53. Xie, T. (2005). Comments on Hong Kong Bill against Unsolicited Electronic Message". November 21, 2005. Retrieved March 15, 2006, from http://www.chinaeclaw.com/News/2005-11-21/4904.html

54. Zeller, T., Jr. (2005, February). Law Barring Junk E-mail Allows a Flood Instead. *The New York Times*, A1.

CHAPTER VII UNSOLICITED E-MAIL WITH ATTACHMENTS

Introduction

The Internet was an outstanding creation of human beings in the 20th century, with its power extending to the current days. More than 683 million e-mail users hold 1.2 billion accounts (Radical Group 2005), and utilize this unprecedented means in communications and marketing. Unsolicited e-mail messages become a nuisance that every user meet by chance. The recipients' property rights, fair trade, public morals, cybersecurity, data protection, and other content-related and goods-related transgresses and offences are all challenges that the society is confronted with (Li 2006).

Many researches have been carried out to analyse the phenomenology of unsolicited commercial e-mail (UCE, or unsolicited business e-mail, UBE, or simply spam). Others have particularly dealt with the costs and benefits of senders and recipients derived from the unsolicited e-mail (Khong 2001, and 2004), the overall impact on productivity of individual employee and enterprises (Nucleus 2003, 2004), the scale and volume of

unsolicited e-mail (Radical Group 2005), the impact on consumers' attitudes and confidence towards e-commerce (TACD 2003; Fallows 2003; Harris Interactive 2003), the higher possibility of receiving unsolicited e-mail by online-published addresses (Federal Trade Commission 2002b), the ignorance of removal requests by senders (Federal Trade Commission 2002a), and the technical and legal solution on unsolicited e-mail (Sorkin 2001).

Few studies have touched with unsolicited e-mail messages with attachments, particularly with how many risks a single e-mail user might be confronted with. In this study, I use a sample of 501 unsolicited e-mail messages with attachment, presenting the first analysis of the types and validity of sender column, types and validity of subject column, types of offers of message content, and types, sizes and nature of attachments of these messages. In this Chapter, the term "spam' is deliberately avoided on the side of the author, due to the lack of a universally-accepted unified definition. At the same time, the author prefers the phrase of "unsolicited e-mail" without the modifier "commercial" or "business", in order to enlarge the coverage of messages with attachments in this study to virus spreaders.

Literature review

As the increase of capability of computers and networks to process information, "a wealth of information" can lead to a "poverty of attention" (Simon 1982). Unsolicited business e-mail (UBE) or unsolicited commercial e-mail (UCE) represents an example that e-mail users must deal with the superfluous information they do not expect to consume.

Unsolicited e-mail brings about the negative image of e-marketing, frightening e-mail users from trusting the e-mail communications.

Unsolicited e-mail sent out to multiple recipients has broad negative effects on e-mail marketing. Karnell (2002) found that an increasing numbers of e-mails have never been read by the recipients, and the users prefer limiting or disrupting the business contacts. The prevalence of unsolicited messages demonstrates a growing threat to the information society (World Summit on the Information Society 2003, paragraph 37).

Spammer-X (2004) told his/her story about the reasons and methods of spamming, revealing the wisdom of defeating anti-spam techniques, avoiding being identified, and escaping the law. McWilliams (2005) described the world of the spammers and spam-fighters, giving information on the mechanisms of spamming and spam fighting. Goodman (2004) presented the most usual spam traps and explained why the current solutions are ineffective. Lambert (2003) analysed a wide variety of e-mail in order to produce a profile of spam and develop a profile of spammer.

The United States Federal Trade Commission (1998) identified a dozen of most likely spam scams, covering spam and scams from business opportunities, quick money, working at home, to guaranteed loans, and so on.

Li (2006) summarized six challenges that the spam brings to the society: the recipients' property rights, fair trade, public morals, cybersecurity, data protection, and other content-related and goods-related transgresses and offences. From the standpoint of the senders, all these challenges could be classified into two bigger categories: victim seeking and conspirator seeking. From the standpoint of the recipient, they are confronted with initial victimization (being spammed), further

victimization (being defrauded, or attacked by viruses), or committing offences (tax evasion, or use of falsified documents).

Nucleus (2003) reported the in-depth interviews with 117 employees and extensive interviews with 28 IT administrators. They found that an average of 13.3 unsolicited messages reached the employee per day; each employee has to spend an average of 6.5 minutes per day dealing with unsolicited messages. The calculated that unsolicited messages caused an average 1.4 percent of productivity loss per employee per year, equal to an average cost of 874 dollars per employee per year.

Nucleus (2004) reported further interviews with employees at 82 Fortune 500 companies. They found that users received an average of twice the number of previous year’s unsolicited messages, with an average 3.1 percent of productivity loss in 2004. They also found that the role of technical solution to unsolicited messages became less effective.

Fallows (2003) reported the Pew Internet & American Life Project, which collected data from a national telephone survey of 2,200 adults and a compilation of more than 4,000 first-person narratives about unsolicited messages. The findings showed unsolicited messages caused some e-mail users to use e-mail less, and trust the online environment less. Fear of unsolicited messages increased.

Federal Trade Commission (2002a) tested 215 addresses from spam with “remove me” claims, and found that 135 removal links or addresses were dead or did not function, attempts to send reply e-mail messages were in the same way unsuccessful.

Federal Trade Commission (2002b) put 250 new, undercovered e-mail addresses in 175 different locations on the Internet, including web pages, newsgroups, chat rooms, message boards, and online directions for web pages, instant message users, domain names, resumes, and dating

services. They found that web pages, newsgroups, and chat room are all attractive to unsolicited message senders.

Federal Trade Commission (2003a) reported that 66 percent of spam messages are fraudulent in the “from” or subject columns, or in the message itself. The false advertisements might distort the normal market of goods and services, harm the normal trade order, and reduce the consumers’ confidence (The Directorate General of Telecommunications Ministry of Transportation and Communications 2005, pp. 6-7). The large volume of spam, the malicious programs and malicious linkages contained in the messages are the main threats (PC World 2003).

Federal Trade Commission (2005) found that spammers continue to harvest email address posted on web sites, and to a much lesser extent, those posted on blogs and USENET groups. Masking email addresses when posting on web sites can substantially reduce the risk of harvesting.

Harris Interactive surveyed 2,376 adults online in 2003, and found that most online adults reported that they received more spam than six months earlier. Only 14 percent have seen a decline in the volume of spam. A majority of respondents reported unsolicited messages annoying or very annoying (Taylor 2003).

Many spammers send their messages by unauthorized use of other individuals or organizations’ accounts (Organization of Economic Cooperation and Development 2004). The e-mail addresses harvesting software can collect this information automatically from the web pages (Boldt, Carlsson and Jacobsson 2004, p. 8). Based on the discussions of spyware and on the findings from the two experiments, Boldt, Carlsson and Jacobsson (2004, p. 4) concluded that spyware has a negative effect on computer security and user privacy. Spyware enables for the spreading of e-mail addresses that may result in the receiving of unsolicited e-mail.

Khong (2004) stated that although it is difficult to measure the costs and benefits of the spammer, if the benefit obtained from the activity outweighs the cost, then the spammer would undertake the spamming activity. It follows that if there is one successful commercial transaction, the spammer can realize his or her benefit. The costs that are involved in the spamming can be roughly estimated according to the costs of bandwidth, message sending, and obtaining of the users' address. The costs of bandwidth and message sending are ignorable. According to Sadowsky (2003, p. 55), the spammer can obtain users' e-mail address in the 13 situations. Obviously, the most convenient and least expensive way is to harvest e-mail addresses automatically with specific software. The software is also available from Internet, either being free of charge or with an inexpensive price.

The revenue of spammer from sending message has been found high in a few studies Goodman and Routhwaite (2004). Cobb (2003, p. 2) suggested the concept of "the parasitic economics of spam," meaning that the act of sending a message costs the sender less than it costs all other parties impacted by the sending of the message.

The costs and benefits of the spammed can also be estimated. The costs induced by the spam to the spammed have a wide coverage. They include the waste of the users' time, bandwidth and storage, cost of anti-spam solution, and cost of overloading at the mailbox (Gauthronet and Drouard 2001). The average time and money lost in processing a single message might not be so significant. However, theoretically, the aggregate loss of time and money in aggregate taken in dealing with these messages might be huge (Li 2006). Spam also induces costs of the bandwidth and storage, losses in interruption of services, and anti-spam solutions (Gauthronet and Drouard 2001). The interruption of services is unfortunate for both the providers and users in causing business,

confidence, and other losses. Worldwide revenue for anti-spam solutions will exceed 1.7 billion dollars in 2008 (IDC 2005). If the e-mail address has ever been put on the institution's Web site, or personal homepage, it is highly possibly that the address will be harvested, sold, and abused by senders (Federal Trade Commission 2003b).

Finally, unsolicited e-mail is nothing useful and beneficial to the recipients. From all of the previous studies, it is reasonable to conclude that the recipients undertake pure losses, not only the monetary, but also the psychological (Li 2006).

Methodology

The Chapter presents a case study on unsolicited e-mail messages with attachments, analysing the sender column, subject column, content and attachments of these message. The sample was composed of all the 501 messages with attachments out of a total of about 26,000 unsolicited e-mail messages collected in one e-mail account through honeypot technique during June 2005 to May 2006.

The account has received 26,160 messages in total, with normal messages accounting for 200 in "inbox" and "backup" folders, and 25,960 unsolicited messages in "5000", "attach" and "spam" folders. The 501 unsolicited messages with attachments have been collected in "attach" folder.

In analysing each message, it is necessary to establish a standard to categorise the messages into different types according to their sender column, subject column, content and attachments. The standard to decide

if the sender column is falsified is the name format. The personal name in Chinese is constituted by "family name plus personal name," while in English it is "first name plus surname." The name for an organization is also easy to judge by comparing the name in the sender column with that in the content.

The standard to decide whether a subject column is falsified is relatively relaxed. Because there is only one message labelled with an "AD:" sign, in strict sense all the subject columns of other messages are illegal. However, the emphasis of this Chapter is not to coincide with the legal standard. Rather, it is focused on the analysis of the phenomenon of unsolicited e-mail messages with attachments. The message with "AD:" label, and messages with words explaining the content or having apparent connection with the content are regarded as not falsified. The other messages with the subject column irrelevant with the content, inducing recipient to open the messages, is considered falsified.

The content is categorised according to the offers provided, and the nature of the attachments.

Findings

Types of File Formats of Attachments

In total 501 messages with attachments, three attachments were missing. Other attachments are comprised of 14 kinds of document formats. More than one third of the attachments are "zip" format compressed files, mostly viruses, which represent the most severe threats to the e-mail

users' computer security. Another one third of all attachments are comprised of two categories: approximately one fifth of the total attachments being "gif" format image files, and approximately one sixth being "htm" format documents. This one third is relatively virus free, but includes annoying contents and hyper links. These three kinds of files constitute more than 70 percent of all attachments. Another frequent attachment format is Microsoft Word "doc", which accounts for 8.4 percent of all attachments. Other 10 kinds of document formats are only responsible for approximately 20 percent of attachments, including both viruses and virus free files.

Table 7 Types of File Formats of Attachments

Types of File Formats	Number	Percentage
*.chm	11	2.2
*.com	9	1.8
*.doc	42	8.4
*.exe	13	2.6
*.gif	92	18.4
*.htm	78	15.6
*.jpg	13	2.6
*.mid	3	0.6
*.pif	19	3.8
*.rar	11	2.2
*.scr	12	2.4
*.txt	8	1.6

*.xls	3	0.6
*.zip	184	36.7
Attachment missing	3	0.6
Total	501	100

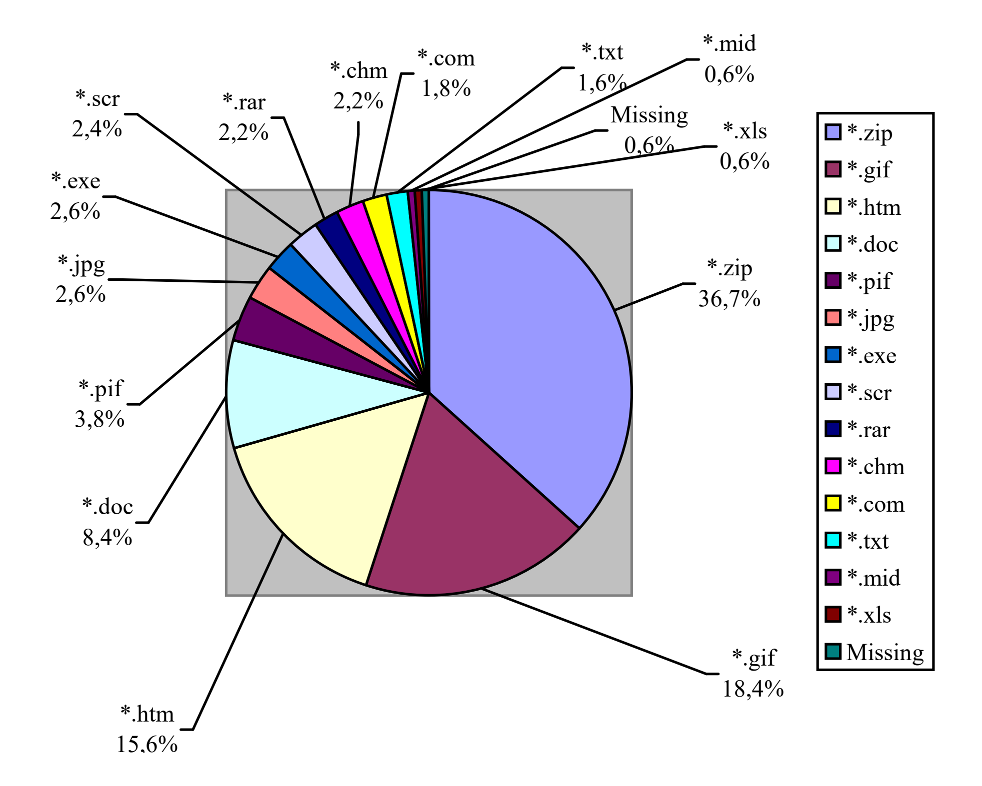


Figure 1 Types of File Formats of Attachments

Sizes of Messages with Attachments

The average size of 501 messages with attachments is 47.44k. The sizes of approximately 90 percent of messages with attachments are smaller than 100k. The sizes of only 2 percent of these messages are between 100-200k. Sizes of nearly 9 percent of messages are bigger than 200k. In fact, about 285 pieces of messages, which constitute more than half of the messages

with attachments, are smaller than 30k. The messages with the sizes of 1k and 2k alone, account for more than 28 percent of the sample. They are mostly empty “zip” files, with the possibility of being messages with attachments of viruses but disinfected by the e-mail service provider. The messages with attachments spreading W32.netsky.C@mm (35k) and W32.Sober.X@mm (75) viruses account for 16 percent and 7 percent of all of the messages respectively.

Table 8 Sizes of Messages with Attachments

Size	Numbers	Percentage
-100kb	446	89.0
100-200kb	11	2.2
200kb-	44	8.8
23,765kb	501	100
Among which		
-30kb	285	56.7
1kb	13	2.6
2kb	108	21.6
35kb	80 W32.Netsky.C@mm	16
75kb	35 W32.Sober.X@mm	7

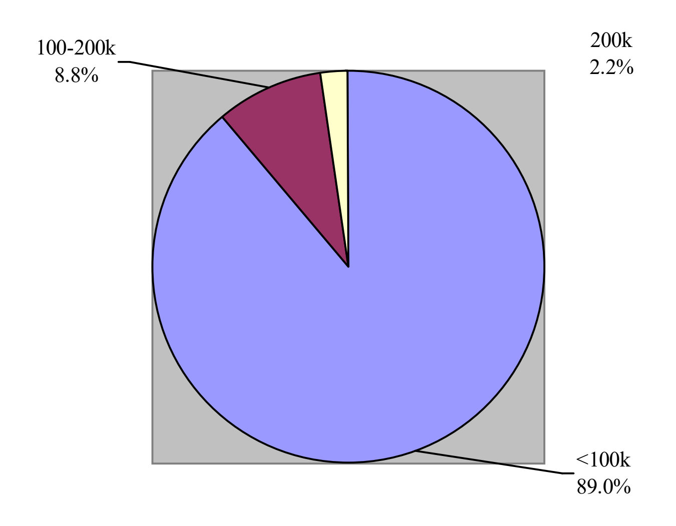


Figure 2 Sizes of Messages with Attachments

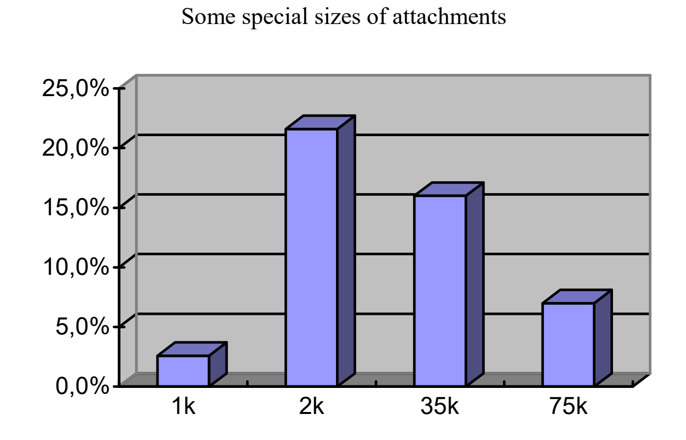


Figure 3 Percentile of Some Special Sizes of Messages with Attachments

The unsolicited messages with attachments account for less than 2 percent of all unsolicited messages. The average size of unsolicited e-mails with attachments is 47.44k, compared with the average size of 7.32k of other unsolicited e-mails, a 6.5 fold bigger. In fact, unsolicited messages with attachments contribute to more than 10 percent of the average message size of all unsolicited messages, enlarging the average size from

7.32k of unsolicited messages without attachments to 8.09k of all of the unsolicited messages.

Table 9 Compare of Average Sizes of Messages

	Total size	Numbers	Average size
Average size of unsolicited e-mails with attachments	23,765k	501	47.44k
Average size of other unsolicited e-mails	186,254k	25,459	7.32k
Average size of all unsolicited e-mails	210,019k	25,960	8.09k
Average size of non-spam e-mails, both with and without attachments	14,892k	200	74.46k
Average size of all e-mails	217,700k	26160	8.32k

Comparatively, the average size of 200 pieces of non-spam messages is 74.46k, even bigger than average size of the unsolicited messages with attachments. The big average size of non-spam messages does not imply that these messages are always bigger than spam messages. It must be pointed out that the fact behind this figure is that the large free space of the e-mail service is used to deposit the users' own backup files, as attachments of self-sending self-receiving messages. A single attachment can be as big as 10Mb with this e-mail account.

Types of Sender Column in Unsolicited Messages with Attachments

Among the 501 pieces of messages with attachments, one is with a blank sender column. Senders of unsolicited messages with attachments tend to hide their names but show e-mail addresses, valid or false. Approximately 60 percent of all messages show e-mail addresses instead of senders' name, which should be considered substandard. Others conceal their names with their surnames and titles, meaningless letters and numbers, describing their offers (products, services and activities), filled with words inducing users to open the messages, or simply exploiting recipients' names and e-mail address. In total, approximately 83 percent of messages bear substandard sender columns. Only around one sixth of messages bear standard personal names or company names.

Table 10 Types of Sender Column in Unsolicited Messages with Attachments

Type	Number	Percentage (/501)
Blank	1	0.2
Company name	45	0.9
Describing products, services and activities	16	3
Inducing users to open the messages	7	1.4
Meaningless letters and numbers	23	4.6

Recipients' name and address	4	0.8
Showing e-mail address	297	59.3
Standard personal name	79	15.8
Surname plus title	29	5.8
Total	501	100

Valid Sender Column in Unsolicited Messages with Attachments

Senders of unsolicited messages with attachments that are currently empty, or with the content of offering banking or financial services, sales of falsified certificate, human resources recruitment, publishing and printing, sales of health products and clothes, soliciting friends, and with the purpose of merely spreading computer viruses are reluctant to provide sender names in standard formats. Senders of unsolicited messages with attachments who offer telecommunications services are also quite reluctant to do so. Approximately one in every three senders of messages with attachments offering information on companies and websites, sales of books, VCD and DVD provide valid name format in sender column. Half of quick money opportunities providers type right names in their messages' sender column. Senders of messages with attachments that offer tax evasion assistance seem more active in provide standard format of names in the sender column. More than half of them did so. Sixty percent of senders who offer information on training and education opportunities type names in standard format in the sender column. The providers of computer hardware and software appear the most reliable senders of

unsolicited messages with attachments, of whom more than 70 percent furnished standard sender column. One quarter out of the senders who offer other services gave valid form of names.

Table 11 Valid Sender column in Unsolicited Message with Attachments

Type	Number of validity in sender column	Percentage
Banking, financial	0	0
Empty attachments	0	0
Falsified certificate	0	0
Human resources recruitment	0	0
Introduction of company, website	6	33.3
Political propaganda	14	56
Publishing, printing, card manufacture, etc.	0	0
Quick money	1	50
Sales of books, VCD, DVD	4	36.4
Sales of health products, clothes	0	0
Software, computer products	33	70.2
Soliciting friends	0	0

Tax evasion	37	53.6
Telecommunications services	1	3.4
Training and education	6	60
Virus	0	0
Other services	1	25

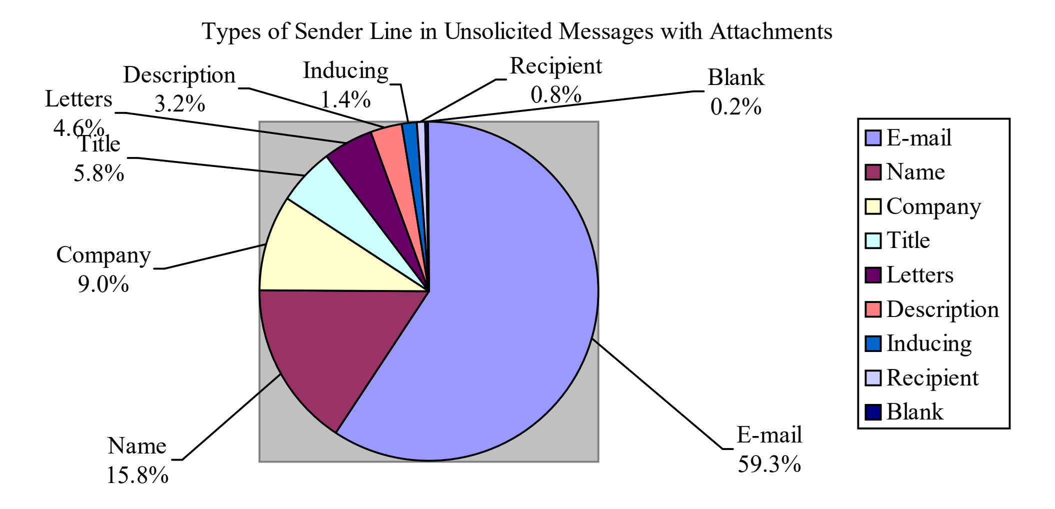


Figure 4 Types of Sender Column in Unsolicited Messages with Attachments

Types of Subject Column in Unsolicited Messages with Attachments

To label the subject column with “AD:”, “ADV:”, or any other kinds of regulatory means, is an invention that has never been respected by senders of unsolicited messages. Only less than two in one thousand messages have this kind of label been stuck. Two in one hundred of the messages with attachments left the subject column blank. Approximately 15 percent of messages used ambiguous languages to confuse the

recipients. All others attempted to draw recipients' attention and attract them to open the messages, furnished the subject column with languages describing the content, giving greetings, appearing related to users' e-mail service, bearing "Re:" and "Fw:" labels, or pretending users' friends and contacts, etc.

Table 12 Types of Subject Column in Unsolicited Messages with Attachments

Type	Number	Percentage
"AD:" label	1	0.2
Ambiguous language	74	14.8
Blank	10	2
Describing message content	117	23.4
Greetings	58	11.6
"Re:" and "Fw:" label	21	4.2
Related to users e-mail service	84	16.8
Special language to draw attention	13	2.6
Users' friends and contacts	123	24.6
Total	501	100

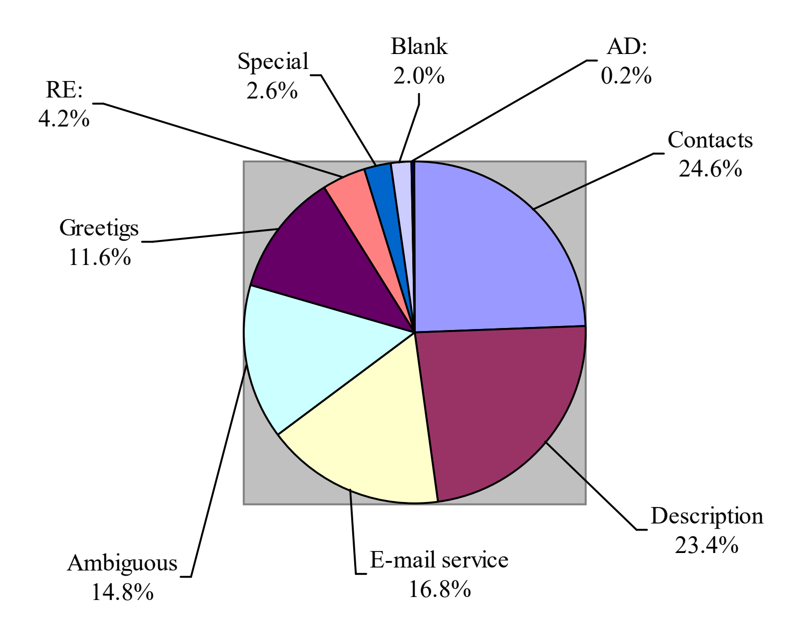


Figure 5 Types of Subject Column in Unsolicited Messages with Attachments

Valid Subject Column in Unsolicited Messages with Attachments

Almost all of the senders of messages with attachments offering information on human resources recruitment, companies or websites, publishing, printing, card manufacture, etc., sales of health products, clothes, and tax evasion ensured the valid subject column. A high percentage of providers of telecommunications services, sellers of books, VCDs, and DVDs, training information providers, quick money information providers, and providers of other services provided valid subject columns in their messages. All the senders of other messages were reluctant in typing useful subjects for their potential recipients.

Table 13 Valid Subject Column in Unsolicited Messages with Attachments

Type	Number of validity in sender column	Percentage
Bank, financial	0	0
Empty attachments	11	10.7
Falsified certificate	0	0
Human resources recruitment	2	100
Introduction of company, website	18	100
Political	1	4
Publishing, printing, card manufacture, etc.	19	100
Quick money	1	50
Sales of books, VCD, DVD	8	72.7
Sales of health products, clothes	4	100
Software, computer products	1	2
Soliciting friends	0	0
Tax evasion	66	95.6
Telecommunications services	24	82.8
Training	7	70
Virus	0	0

Other services	3	75

Types of Content of Messages with Attachments

More than 28 percent of messages are designed to spread viruses. More than one in five messages attached empty attachments. Messages offering both tax evasion services and software and computer products constitute around 10 percent of all messages. Any of contents of other messages constitute a percentage far below 10 percent, with messages offering telecommunications services and political propaganda constitute around 5 percent separately. Interestingly, there is rarely any message with attachment involving adult contents, investment chances, sales of pirated software, and some other common offers in messages without attachments found in the same e-mail account.

Table 14 Types of Content of Messages with Attachments

Type	Number	Percentage
Bank, financial	3	0.6
Empty attachments	103	20.6
Falsified certificate	10	2
Human resources recruitment	2	0.4
Introduction of company, website	18	3.6
Political	25	5
Publishing, printing,	19	3.8

card manufacture, etc.		
Quick money	2	0.4
Sales of books, VCD, DVD	11	2
Sales of health products, clothes	4	0.8
Software, computer products	47	9.4
Soliciting friends	4	0.8
Tax evasion	69	13.8
Telecommunications services	29	5.8
Training	10	2
Virus	141	28.1
Other services	4	0.8

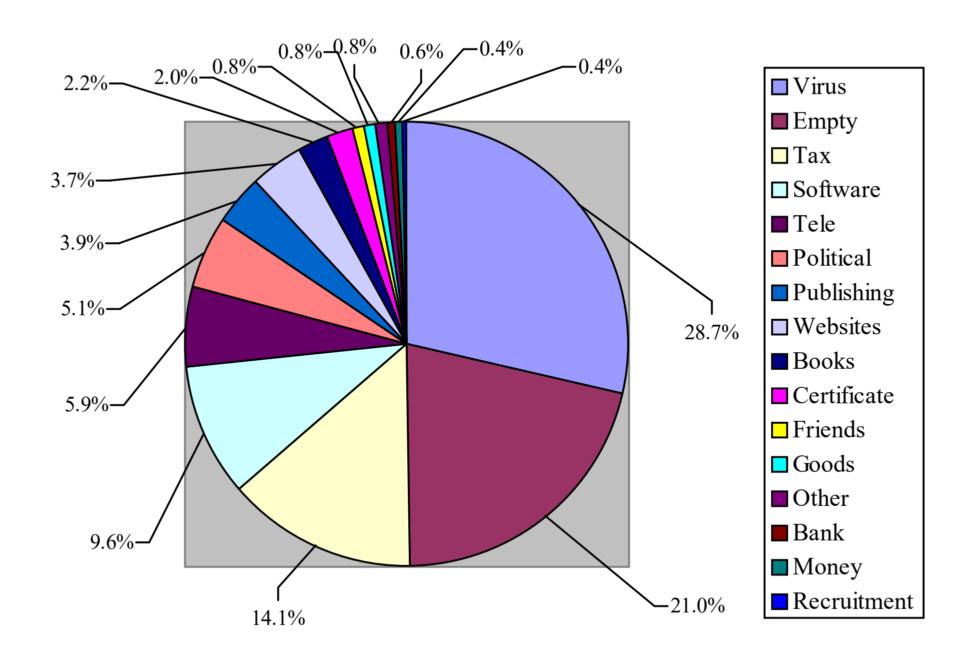


Figure 6 Types of Content of Messages with Attachments

Valid Content in Unsolicited Messages with Attachments

Interestingly, most messages have high percentage of valid contents, with the exceptions of messages with empty attachments and messages with attachments that spread viruses.

Table 15 Valid Content in Unsolicited Messages with Attachments

Type	Number of validity in content	Percentage
Bank, financial	0	0
Empty attachments	0	0
Falsified certificate	9	90

Human resources recruitment	2	100
Promotion of company, website	13	72
Political	25	100
Publishing, printing, card manufacture, etc.	19	100
Quick money	1	50
Sales of books, VCD, DVD	11	100
Sales of health products, clothes	4	100
Soliciting friends	4	100
Software, computer products	47	100
Telecommunications services	24	82.8
Training	8	80
Virus	0	0
Other services	1	25

Types of Contact Method Provided in Unsolicited Messages with Attachments

Because many unsolicited messages with attachments are spreading viruses, they generally provided no contact information, with a few exceptions. Other messages included one or more kinds of contact methods

in the message texts. Of total 501 messages, more than one-third of the messages provided hyperlinks directed to websites, while less than one-third provided fixed telephone numbers. Both e-mail addresses and mobile phone numbers are preferred by more than 22 percent of senders. Fax numbers and physical addresses are included in about 16 and 10 percent of messages separately. QQ (a chat system mainly used by Chinese Internet users) are provided in 8 percent of messages. MSN is the least used contact method in the 501 messages.

Unsubscribe is nothing more than a decoration in unsolicited messages with attachments. Unsubscribe method is only provided in 2.2 percent of messages.

Table 16 Types of Contact Method Provided in Unsolicited Messages with Attachments

Contact Methods	Number	Percentage (/501)
Address	50	10
E-mail	113	22.6
Fax	79	15.8
MSN	12	2.4
Mobile phone	112	22.4
QQ	40	8
Telephone	145	28.9
Unsubscribe method	11	2.2
Website	182	36.3

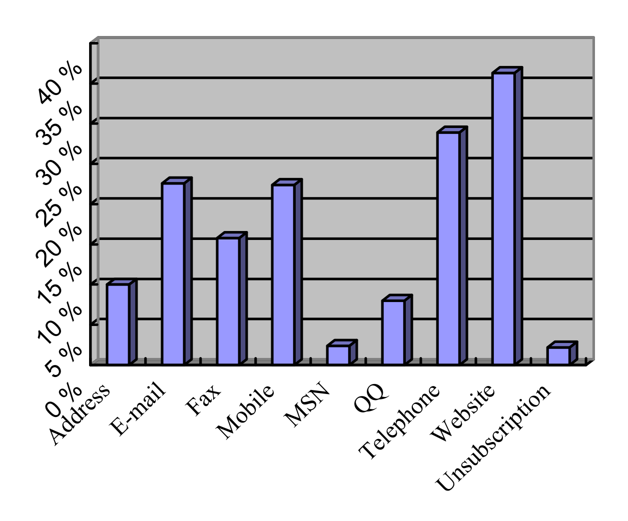


Figure 7 Types of Contact Method Provided in Unsolicited Messages with Attachments

Falsity of Sender, Subject and Content

Only one in five of the unsolicited messages with attachments used valid format in sender column, one in three used valid subject column, and more than half provided valid content. However, only 58 messages had both valid format of sender and subject column, and 293 messages with both false format of sender and subject column. Other 42 messages have valid format of sender column but false format of subject column, while 108 messages have false format of sender column but valid format of subject column. The overall falsity of subject or sender column constitutes 88.4 percent.

Table 17 Validity and Falsity of Sender and Subject Columns and Content Separately

		Number	Percentage

Sender	Valid	100	20
	False	401	80
Subject	Valid	166	33.1
	False	335	66.9
Content	Valid	260	51.9
	False	241	48.1

The validity and falsity of content take almost 50 percent separately.

Table 18 Validity and Falsity of Either Subject or Sender Column

		Sender			
		Valid	False	Total numbers	Percentage
Subject	Valid	58	108	166	33.1
	False	42	293	335	66.9
	Total numbers	100	401	501	100
	Percentage	20	80	100	
	Percentage of validity of both columns	11.6			

Discussion

Senders of e-mail messages with attachments adopted adept tricks in attention getting and trepanning the recipients. Opening the messages and the attachments is the first goal of the senders. Generally, they use ambiguous and false sender and subject columns, but ensure the valid contents (except messages spreading viruses) so as to show their offers and set their traps.

The surveyed messages with attachments prove that, except messages spreading viruses, they are relatively moderate in the sense of harmfulness of the contents, compared with the findings in the previous studies that did not distinguish messages with attachments from those without.

At the same time, this study reveals that the unsolicited e-mail messages with attachments can have broader influence on the criminal phenomenon, not only victimization, but also conspiracy. This exploits the function of e-mail communications being an offensive means by which the recipients are victimized as well as being a conspiracy tool with which the recipients are seduced to participate criminal operations.

In the Internet environment, the most frequent victimization model begins from exposing of victims to the potential threats, which we can call as exposing-victimization model. Under this model, the victim of unsolicited messages with attachments merely puts his/her e-mail address on the web pages, bulletin board systems, uses it in the chat systems, or even only transmits it through the Internet. The exposure does not necessarily mean show-off. Rather, it is just a kind of presence on the Internet literally or digitally, something inevitable. Nevertheless, the exposing-victimization model at least implies that the senders of unsolicited messages with attachments could easily get the e-mail address

in the same way as other Internet users do, without further efforts in collecting or harvesting these addresses.

In other cases, the senders of messages with attachments have a seeking process, and follow the seeking-victimization model. Due to the large quantity of web pages and other Internet-related contents, the direct artificial collection of multiple e-mail addresses becomes inefficient. The senders (here we also imply address providers) utilize specialized software to harvest e-mail addresses from the Internet. The collecting process becomes automatic and efficient. By doing so, they created the seeking-victimization model in sending messages with attachments. Besides harvesting, they also exploit dictionary attack and/or automatic alphabetical permutation and combination to enumerate possible usernames in e-mail accounts. These methods can also be categorised into seeking process. For the senders, an e-mail account with a random word might not represent a specified person; but for the recipient, he/she is readily the victim of this unsolicited message with attachment.

The victimization of recipients of unsolicited messages with attachments happens without the appearance of the recipients in their e-mail account. The victimization means that their e-mail accounts are being spammed, whether they open their accounts or not. Under current legal framework, the receiving of unsolicited messages is sufficient to constitute victimization of the behaviour to be imposed punishment.

However, the victimization of unsolicited messages with attachments does not end at the initial victimization. The above-mentioned models could be called as the first level effects of unsolicited messages with attachments. Subsequently, the second level effects are based on the initial victimization. There are possibly also two models: initial victimization-subsequent victimization model and initial victimization-conspiracy model.

The initial victimization-subsequent victimization model happens when the messages include viruses, fraudulent sales of goods, or falsified financing and banking services. The first level victimization is being spammed, while the second level victimization is being attacked or swindled.

The second level victimization does not always fulfil so simply. There usually involves an initial victimization-exposing-seeking-subsequent victimization process. In the case of the Nigerian fraud (or 419 fraud), the recipients of the unsolicited messages are firstly victimized by receiving this kind of messages (being spammed). If they make positive reaction to the messages, they are further exposing to the senders. Upon receiving the recipients' reaction, the senders will further seek the vulnerability of the recipients and the possibility of obtaining their property. The process of seeking and exposing might be repeated for a number of times. If the senders succeed in obtaining the recipients' property, the last victimization would happen and the scam would end.

The victimization-conspiracy model happens when the messages include tax evasion services, sales of pirated software, sales of falsified documents, and so on. The recipients of such offers are firstly victimized by the unsolicited messages; and if they participate the illegal operations, they would become the conspirators of the senders.

Because the recipients of the unsolicited messages inducing conspiracy in an illegal operation would expect to benefit from the cooperation with the senders, the senders are more likely to send this kind of messages. In fact, in Nigerian fraud, the senders are usually personating politicians who want to transfer property (money, diamond, and so on) to the bank accounts of the recipients. As a result, the "conspirators" of money laundering are finally to be victimized in the trickery.

Conclusion

The phenomenon of unsolicited e-mail messages with attachments further proved the low controllability or uncontrollability of the information network environment. Any e-mail address is vulnerable to unsolicited messages that were sent to exposed accounts on the Internet or supposed account according to the dictionary. For the senders, both ways could be seen as a process of seeking. For recipients, both ways could also be seen as a process of exposing. However, these seeking and exposing processes have become more abundant and colourful in the Internet environment than pre-Internet times.

The mere browse of the web pages is the easiest method to get e-mail account, but it is less efficient. The sender can also purchase millions of addresses of different interests of users from the specific vendors. Except an inexpensive price, the buyer can conveniently reach a majority of these addresses. Besides, the address harvesting becomes automatized and prevalent with the help of powerful software. Anyone with a few computer and Internet knowledge has the ability to master the uncomplicated skills and subsequently collect thousands or millions of addresses with specific software, which can be downloaded from the Internet free of charge or with a small payment.

The exposure of e-mail account on the Internet is unavoidable, because the exposure is in so broad a sense that all the normal use of the account could be seen as an exposing process, including sending and receiving messages; publishing on web pages, chat rooms, and BBSes; providing as register information in online services; or exposing nothing

more than coincidence with a dictionary vocabulary; or merely permutation and composition of letters and numbers that the senders also dope out. In fact, exposure of a single e-mail account will not be so risky without the harvesting mechanism, because it is an inefficient way to pick up single e-mail account from the Internet. However, because the e-mail account vendors could collect and transfer in a dynamic process, and finally form a growing account database to maintain their business. The harvesting software and dictionary attack undoubtedly deepen the victimization of the e-mail account holders.

In general, the exposed e-mail account might face double risks of being victimized: being collected in formal browse of web pages and use of other Internet services; and being harvested and guessed. Compared with daily used e-mail accounts without showing up on the web pages or other Internet services except merely sending and receiving messages, the published accounts are more likely to be victimized. Therefore, it seems more likely that the process of harvesting but not guess that feeds on the vendors of database of e-mail accounts and senders of unsolicited messages. As a result, the double risks of exposed e-mail accounts are in fact unbalanced: the risk of being victimized by collectors and harvesters are far serious than the guessers.

The unsolicited messages with attachments provide e-mail users many different choices, either legitimate or illegitimate, either to conspire or to be further victimized by attached viruses or pre-established fraud traps. The majority of messages in this study granted recipients two alternatives: to conspire in tax evasion, or to be damaged by viruses.

In the case of conspiracy in tax evasion, the senders always provide valid contact methods so as to induce the recipients to participate in the illegitimate operations. The offer seemingly aims to establish a relationship between service provider and clients. But the effect is that

they form conspiracy. The recipients have to react actively before they become the conspirators of the tax evasion activities. The process might involve repeated e-mail exchanges upon the initial unsolicited messages. Under these circumstances, the unsolicited messages might be transformed into literally valuable (but morally wrong and legally prohibited) information. Such messages become the communications means for the trespassers and criminals, posing great threats for the social control over illegal activities.

In the case of viruses attack, the senders exploited social engineering to induce the recipients to open the messages and subsequently the attachments, by blurring the sender, subject columns and falsifying the message contents and attachment names. These messages do not require replies from the recipients before they cause damages. They are also dangerous for the recipients in the sense that they are harming the recipients' hardware and software, wasting the labour force, and hindering the business.

References

1. Boldt, M., Carlsson, B., & Jacobsson, A. (2004). Exploring Spyware Effects. Retrieved 31 May 2006, from http://psi.bth.se/mbo/exploring_spyware_effects-nordsec2004.pdf
2. Cobb, S. (2003). The Economics of Spam. Retrieved 31 May 2006, from http://www.spamhelp.org/articles/economics_of_spam.pdf
3. Fallows, Deborah (2003, October). Spam: How It Is hurting E-mail and Degrading Life on the Internet. Retrieved 31 May 2006,

from http://www.pewinternet.org/pdfs/PIP_spam_Report.pdf

4. Federal Trade Commission (1998, July). Federal Trade Commission Names Its Dirty Dozens: 12 Scams Most Likely to Arrive via Bulk E-mail, *Federal Trade Commission Consumer Alert*.
5. Federal Trade Commission (2002a, April), *Remove Me Surf*.
6. Federal Trade Commission (2002b, November), E-mail Address Harvesting: How Spammers Reap What You Sow.
7. Federal Trade Commission (2003a, April), *False Claims in Spam: A Report by the Federal Trade Commission's Division of Marketing Practices*.
8. Federal Trade Commission (2005). Email Address Harvesting and the Effectiveness of Anti-Spam Filters: A Report by the Federal Trade Commission's Division of Marketing Practices, November 2005.
9. Federal Trade Commission. (2003b, June 15). *National Do-Not-E-mail Report to Congress*.
10. Gauthronet, S., & Drouard, E. (2001). *Unsolicited Commercial Communications and Data Protection*. Brussels: Commission of the European Communities, Internal Market Directorate General.
11. Goodman, Danny (2004), Spam Wars: Our Last Best Chance to Defeat Spammers, Scammers & Hackers, New York, New York: SelectBooks.
12. Goodman, J. T., and Rounthwaite, R. (2004). Stopping Outgoing Spam. In: *Proceedings of the 5th ACM Conference on Electronic Commerce*, 17-24 May, ACM Press, pp. 30-39.

13. IDC (2005, February 24). Worldwide Revenue for Antispam Solutions To Reach Over $1.7 Billion in 2008, IDC Reveals. *IDC - Press Release.*

14. Karnell, J. (2002). Raising the Stakes in Permission Marketing. Retrieved 31 May 2006, from http://www.onetooneinteractive.com/resource/whitepapers/0003.html

15. Khong, W. K (2001, October). The Law and Economics of Junk E-mails (Spam). Retrieved 31 May 2006, from http://www.frg.eur.nl/rile/emle/Theses/Khong.pdf

16. Khong, W. K. (2004). An Economic Analysis of Spam Law. *Erasmus Law and Economics Review*, 1 (February), 23–45.

17. Lambert, Anselm (2003, September). *Analysis of Spam*. Master of Science in Computer Science Dissertation, Dublin: University of Dublin.

18. Li, X. (2006). E-Marketing, Unsolicited Commercial Electronic Mail, and Legal Regulations, *Webology*, Vol. 3, No. 1, 2006.

19. McWilliams, Brian (2005). *Spam Kings*, Sebastopol: O'Reilly Media.

20. Nucleus (2003). *Spam: The Silent ROI Killer*, Research Note D59.

21. Nucleus (2004). *Spam: The Serial ROI Killer*, Research Note E50.

22. Organization of Economic Cooperation and Development (2004). *Second Organization of Economic Cooperation and Development Workshop on Spam: Report of the Workshop.*

23. Organization of Economic Cooperation and Development (2003). *Organization of Economic Cooperation and Development Guidelines for Protecting Consumers from Fraudulent and*

Deceptive Commercial Practices Across Borders, Author.

24. PC World (2003, August 29). Sobig May Be Working for Spammers. Retrieved 31 May 2006 from http://www.pcworld.com/news/article/0,aid,112261,00.asp

25. Radical Group (2005). *The Radical Group, Inc. Release Q1 2005 Market Numbers Update.*

26. Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B. J., and Schwartz, A. (2003). *Information Technology Security Handbook*. The International Bank for Reconstruction and Development.

27. Simon, H. A. (1982). *Designing Organizations for an Information-Rich World: Models of Bounded Rationality*. Massachusetts: Massachusetts Institute of Technology Press.

28. Sorkin, D. E. (2001). Technical and Legal Approached to Unsolicited Electronic E-mail, *University of San Francisco Law Review*, Vol. 35, pp. 325-384. Retrieved 31 May 2006, from http://www.sorkin.org/articles/usf.pdf

29. Spammer-X (2004), *Inside the SPAM Cartel,* Rockland, Massachusetts: Synergies Publishing.

30. Taylor, Humphrey (2003, 10 December). Spam Keeps on Growing. Retrieved 31 May 2006, from http://www.harrisinteractive.com/harris_poll/index.asp?PID=424

31. Trans Atlantic Consumer Dialogue (TACD) (2003). *Consumer Attitudes Regarding Unsolicited Commercial E-mail (Spam).*

32. World Summit of Information Society (2003, December). *Declaration of Principles-Building the Information Society: A Global Challenge in the New Millennium*.

CHAPTER VIII CYBER WARFARE?

Introduction

While we are enjoying the fruits of the possibility of disseminating information in large quantities and at high speed in this networked society, we have also to take the risk of forcing ourselves to trade unexpected by-products of cyberspace. Information and communications technology (ICT) can produce a surprisingly large amount of products and by-products for these technology-dependent people, such as security and insecurity, welfare and crime, peace and war, to name some. In fact, insecurity, crime and war are information society's silhouettes, merging easily but being difficult to eliminate.

Overall, the Internet services lack of controllability and become the breeding ground of insecurity, as a response to which many governments have enacted specific legislation criminalizing invasive and destructive activities targeted at information systems. Because security-breaking activities, committed with the assistance of the globally-connected computer networks, can easily cross the territorial borders, it is unknown but broadly accepted that different countermeasures may generate a

paradise for perpetrators.

Information Warfare (IW) is increasingly listed alongside nuclear, chemical, and biological weapons as a potential weapon of mass destruction (WMD)—or at least as a weapon of mass disruption (Eriksson 1999, pp. 57-64). Under such circumstances, interest in and concern for cyber warfare have also been prevalent for decades. War-oriented writer usually exploited such serious and expensive terms as cyber war, information war, and electronic war to spread their impetuous and cheap ideas. Using search engines, we can produce the following numbers of results (as of July 17, 2009):

Table 19 Online Use of Cyber War Terms

	Google	Yahoo	Amazon (copies of books only)
Cyber war	121,000,000	55,600,000	697
Cyberwar	1,770,000	4,740,000	718
Cyber warfare	840,000	11,100,000	549
Cyberwarfare	315,000	2,890,000	278
Information war	1,140,000,000	875,000,000	26,445
Information warfare	94,800,000	59,100,000	4,594

It may be said that the terms are used in a way blotting out the sky and the earth in cyberspace. Yet worse, authors created scores of books in the title of which filled with such terms as well, mostly without critical views against the abuse of them. Information society, to some extent,

means there is too much information for users to consume, so that they are frightened by cyber war and cyber terror, victimized by cyber bullying and cyber crime, and at last jammed by cyber jokes, cyber hoaxes and cyber hypes.

As a computer and network security researcher and industry leader, Marcus J. Ranum said in March 2009,

"There has been a great deal of irresponsible and inaccurate talk about 'Cyber War' in the last decade in spite of the fact that it's technologically and militarily impractical. Its counterpart, 'Cyber Espionage' makes a bit more sense, and is less mythical but falls under the category of 'nothing new.'"

Nevertheless, there are still few people realizing the real issue behind media's full coverage of cyber attack during big or small international conflicts. No more than a month ago, it was reported that Britain's Security Minister, Lord West, as he published the Government's Cyber Security Strategy, had issued a warning about terrorists' intentions of launching a cyber warfare battle against the UK (Gardham 2009).

The strategy clarified in detail the threats from various actors. Besides criminals,

"The most sophisticated threat in the cyber domain is from established, capable states seeking to exploit computers and communications networks to gather intelligence on government, military, industrial and economic targets, and opponents of their regimes. The techniques used by these state actors go beyond 'traditional' intelligence gathering and can also be used for spreading disinformation and disrupting critical services…Some states also encourage, and benefit from, the expertise of 'patriotic hackers'…carrying out attacks safe from prosecution in their own countries. The use of proxies provides state

actors with an extra level of deniability". (UK Office of Cyber Security and UK Cyber Security Operation Centre 2009, p. 13)

"Terrorists and violent extremists use cyber space for communication, co-ordination, propaganda, fundraising, radicalisation, and recruitment…Whilst we expect terrorist groups to continue to favour high-profile conventional operations over cyber attacks, we must be vigilant against any future increase in capability…" (UK Office of Cyber Security and UK Cyber Security Operation Centre 2009, p. 13).

A growing tendency is that many writers have recognized the pseudomorphism of the cyber warfare hallucination, revealing the truth and interest behind cyber warfare claims. This essay by no means devaluates serious designs and plans, studies and research, ideas and claims revolving around cyber warfare. Rather, the purpose of this Chapter is to analyze existing jokes, hoaxes and hypes on the so-called cyber warfare, so as to distance serious research from misleading information. Serious researchers should always bear in mind that the use of information on cyber warfare in today's world is a thing that needs reliable evidence, proof and witnesses.

How to write "the scariest cyber warfare article"

Cyber warfare as become a big topic, an attractive topic, a revenue-generating topic, and a hot topic. Readers and audience are willing to read, listen and watch however it is written, narrated and performed. Authors are willing to write whatever the readers are willing to read. Media are willing to publish whatever the authors are willing to write and whatever the readers are willing to read. Every player meet his/her own needs in

one way or the other: readers satisfy their endless curiosity by reading, writers make their money by writing, and media win both popularity and money from publishing, and government show up its political achievements. Even the army will demonstrate their ability and capacity by presenting their understanding of and deal with the "big" issue, which is something a mystery for layman. However, any discourse has to have some structural expression, beginning with attraction, processing with ambiguity, and ending with suspense. Yet everything should not be so accurate, so sound, so clear, and so sure.

Therefore, when we read almost all of the news reports and articles by non-academic authors, we have the strong feeling that these articles can be composed by everyone who is willing to do so. Reality, fact, truth, accuracy and conscience are not so relevant here. The only things are some tips that should be followed. Evgeny Morozov published his guidance on "10 easy steps to writing the scariest cyber warfare article ever" (Morozov, 2009a). There, he sarcastically proposed some tips on how a cyber warfare article can be manufactured. Key things to be presented are: digital Pearl Harbor, 2007 attacks on Estonia, Chinese hackers, cyber-pranks, expert quotations, old stories, etc. By doing so, a cyber warfare article can be concocted in a low-cost high-benefit efficient way.

His steps are (seemingly only 9 steps, with original step 7 missing. Here they are re-numbered):

1. Give a catchy title with coined terms such as "digital Pearl Harbor", "cyber-Katrina", and "electronic 9/11", but never explain what it means;

2. Begin the story with 2007 attacks on Estonia, but never mention that it only lasted for twenty minutes;

3. Drop references to Chinese hackers in every paragraph;

4. Mention the cyber-pranks of Kremlin-affiliated youth movements;

5. Find and quote industry experts with the biggest possible conflicts of interest;

6. Go and recycle old facts, quotes, and official statements;

7. Throw in some geopolitical kerfuffle that involves a country located between China and Russia;

8. Refer to anything involving cyber war between Israel and Palestine;

9. Make sure to mention that NSA, CIA, and DIA are all involved in the case, but they cannot comment.

In a word, writing about cyber warfare could not be done by delicate scientific calculation, detailed statistics, real-life interview, deep investigation, and field work in person. It should be developed through imagination under some kinds of inspiration. It is like a sci-fi rather than a fact report.

Practically, among others, every article published in recent three years began with 2007 cyber attacks on Estonia, which has already been proved to be the act of a native ethnic Russian young man. No nation state was ever involved. No government was behind him. No official coordination ever took place. Yet they suspected a country from beginning to the end. Furthermore, authors tend to connect every catastrophic result in critical infrastructure in the real world with possibility of interruption of the Internet. As typical articles started the narration in this way:

"Imagine that agents of a hostile power, working in conjunction with organized crime, could cause huge traffic jams in your country's biggest cities-big enough to paralyze business, the media, government and public services, and to cut you off from the world. That would be seen as a grave risk to national security, surely? Yes, unless the attacks came over the internet." (Economist, 2007).

"The next world war might not start with a bang, but with a blackout. An enemy could send a few lines of code to control computers at key power plants, causing equipment to overheat and melt down, plunging sectors of the U.S. and Canadian grid into darkness. Trains could roll to a stop on their tracks, while airport landing lights wink out and the few traffic lights that remain active blink at random.

"In the silence and darkness, citizens may panic, or they may just sit tight and wait for it all to reboot. Either way, much of the country would be blind and unresponsive to outside events. And that might be the enemy's objective: Divert America's attention while mounting an offensive against another country." (Derene, 2009)

In fact, events in cyberspace could never be compared with their social counterparts. No one has reportedly died of hacking, spamming or stalking. No company has reportedly bankrupted due to denial-of-service attacks. Even the broadly concerned Nigerian 419 scam has never had as big a business as done by the former chairman of the Nasdaq stock market. It seems that when people are unable to deal with issues in from of them, then they will look for some scapegoat, regardless of offline or online, so that the issue can be enlarged at such a scale that it seems cannot be dealt with using normal efforts. As a result, they are to be excused. Then more sophisticated ideas will be written; what are written will be published; what are published will be read; what are read will surely benefit all. Government and the army will get more money from taxpayers and employ more personnel, construct bigger office buildings, be better respected by citizens. "Cyber warfare" discourse is helping to form a cost-effective new industry. As Morozov pointed out that,

"Cyber-security fears have had, it should be said, one unambiguous effect: they have fueled a growing cyber-security market, which, according to some projections, will grow twice as fast as the rest of the IT industry."

(Morozov, 2009b)

However, look at how media are trying to distance themselves from the author, even though they are pleased to harvest money from fake stories:

"Reader's advisory: Wired News has been unable to confirm some sources for a number of stories written by this author. If you have any information about sources cited in this article, please send an e-mail to sourceinfo[AT]wired.com." (Retrieved July 17, 2009 from http://www.wired.com/politics/law/news/2001/04/43437).

April Fool's joke

In early 1990s, during Gulf War I, Infoworld magazine published as April Fool's joke. The story claimed that the National Security Agency had developed a computer virus, called AF/91, to immobilize Iraqi air defense computers by chomping windows. What was mystified was that the virus was smuggled into Iraq through Jordan, concealed in a chip in a printer.

The joke was gossiped for days by those who thought it funny as well as those who missed the original citation and engaged in laborious discussion on the imagined technology of the virus (Smith, 2003). U.S. News and World Report acquired the story and published news of the Gulf War virus in its coverage of the war (Smith, 2003). The U.S. News and World Report wrote that the Gulf War virus attacked Saddam's defenses by "devouring windows" that Iraqi defenders used to check on aspects of their air defense system: "Each time a technician opened a window…the window would disappear and the information would vanish." From there,

the fake story was reported by the Associated Press, CNN, ABC Nightline, and newspapers across the U.S. (Smith, 2003).

In probing the reason why the hoax could succeed, Smith (2003) pointed out that,

“The Gulf War virus plays to a uniquely American trait: a child-like belief in gadgets and technology and the people who make them as answers to everything. Secret National Security Agency computer scientists made viruses that hobbled Saddam's anti-air defense without firing a shot! Or maybe it didn't work but it sure was a good plan!”

Some years later, I heard another piece of news from radio, reporting that there emerged a kind of powerful influenza virus, which could reside in a telephone and spread via the telephone line to other telephones, regardless of however its length was. As soon as the call from the telephone where the viruses resided was accepted by the other side, the viruses could transport themselves along the line to the telephone where they did not yet reside by 300,000 kilometers per second, the velocity of light. It was a matter of picking the phone up. They came out now and then from the telephone they resided and infected people nearby. This humorous version of a horror, integrating both natural phenomena and high-tech invention, can pose a more “realistic” threat against human beings than cyber warfare does. Just imagine it.

Rise and fall of Estonian cyber war hoax

“Estonia, a good place for an alleged cyberwar because no real journalists were actually interested in actually wasting their time in going there to

investigate it, is a fine repeatable tale in the tradition of digital warstories." (Smith 2007)

The term "Estonia under cyber attack" made many people to recall the breaking news broadcast on TV on September 11, 2001, when several planes flew into several U.S. buildings. The difference between them is that the Estonian version is a cyber attack. April of 2007 witnessed Estonian authorities' relocation of the Bronze Soldier of Tallinn from the center of the capital city to the outskirts of town. Nationalists in that country considered the Soviet Red Army as occupiers and oppressors. Ethnic Russians, making up nearly a quarter of Estonia's population, were incensed by the statue's treatment and took to the streets in protest. Estonia later blamed Moscow for coordinating the turbulence; order was restored after American and European diplomatic interventions. Days after the riots, the information infrastructure of Estonia began to fray, victimized by "denial of service" attack. A flood of sham requests for information from computers around the world conspired to cripple the websites of Estonian banks, media outlets, and ministries for days. Estonia denounced the attacks as an unprovoked act of aggression from a regional enemy.

Some observers reckoned that the onslaught on Estonia was of a sophistication not seen before. The case is studied intensively by many countries and military planners as it may have been one of the largest instances of state-sponsored cyberwarfare.

Estonian Foreign Minister Urmas Paet accused the Kremlin of direct involvement in the cyber attacks. However, on September 6, 2007 Estonia's defense minister admitted he had no evidence linking cyber attacks to Russian authorities. Russia called accusations of its involvement "unfounded," and neither NATO nor European Commission experts were able to find any proof of official Russian government

participation.

In early 2008, one Estonian ethnic-Russian national has been charged and convicted. The so-called Estonia Cyber War turned out to be some Estonian citizens' activities. What an embarrassment for all those who had ever hyped such a case as a cyber war.

A "cyber warfare" years before

According to many journalists and analysts, "Cyberwar has always been said to be easy to do. Al Qaeda has always been said to be working on it. Before al Qaeda, it was Russia, China, India, North Korea. Even Saddam Hussein was imagined to be readying a US-smashing Internet strike force." (Smith 2007)

In recent years, the so-called cyber warfare becomes a routine activity when ever international conflicts emerge. One of such occasion took place in 2001 when the world was in troubled times. Early that year, a scholar had launched a "cyber war" by himself and he was nearly criminally investigated. At the time, He was offered a scholarship to pursue studies and research on economic criminal law in a highly industrialized country, where the computer and networks had already been ubiquitously used. His office there was equipped with a computer and it got connected to the Internet.

Long before that, he had had some interest in doing further research on cybercrime, the counterpart of which, computer crime, had been the theme of his master's degree thesis.

Lawyers whose research was focused on legal issues in cyberspace

generally did not probe the mechanism of these activities in detail. In this occasion, in order to better understand how the computer could be compromised, he decided to do a series of experiments. He made contact with some laboratories in West Europe and North America for potential opportunities to be hosted, but only in vain. Finally, he began to change his office into his own laboratory, using two notebook computers. The first step of his experiment was to test the security level of computers in several universities and other institutions in several countries located in different continents, so that he could have first-hand knowledge about whether they were protected and to what extent they were secure. The experiment was done by using programs publicly available on the web. No one said whether such tools were legal or not. No one prohibited them from being created and disseminated. He just used such tools in his experiment to look for externally accessible computers online. Upon setup the parameters, the work was automatically done, with open ports listed. During a time span of around 10 days, he used his computers at work in day time, and left them doing the research in night time.

He took down each open vulnerable computer in a note book. After some days, hundreds of thousands of computers had been tested; hundreds of such computers had been found, including those in use at universities in that country and other countries. By this record, he could do quite a lot of analysis.

His work would have never been completed voluntarily as the result would surely have been of great value for his research.

However, all of a sudden, his computers were taken offline by the computer centre of the host university, and an investigation was set out firstly by a professor at the same faculty, who also did research on informatics.

According to the IP address assigned to me in advance, he visited his office and had a brief look at his laptops. He just confirmed that the suspected IP address was that had been used in the suspected attack.

As a response, he paid a visit to the professor's office soon after and explained his awkward work during the past days. The professor had opened an email message on his desktop screen, saying that the computer centre had noted abnormal activities from a computer with a certain IP address, which should have been assigned to a user at this faculty. The influence of this was that the abnormality exploited quite some the then scarce bandwidth and the network connection at this university became slow. Then the computer centre requested the professor's assistance with the investigation. The professor was the just person he gave his confession and showed his record of "open ports" from some top universities. Besides, the professor had a proof for his motive in the form of a manuscript of an article.

The university's computer centre was once concerned with his act. But after the professor understood all he had done, the professor told him two points:

1. Stop his experiment immediately even if it was useful for me;

2. Let him ensure no actual access to any computer and investigation would concluded, and no worry.

He was fortunate as his experiments were understood by a professor who knew both computer science and law; and the computer centre was so wise, nice and kind that they didn't take the matter for granted as a crime or a war. He was not an offender, nor a warrior.

Many others were not as lucky as him. In approximately the same season, a student at another university was found guilty of using a computer doing similar things as his, accessing several computers in that

country, revising data or even programs in them. That student's case was investigated by criminal police and he made real trouble with his computer. He might have not given as perfect an explanation about his work as the scholar had about mine. Thus he might well be regarded as a cyber offender, or a cyber warrior, or even a cyber spy. A long judicial procedure and investigation were waiting for him, enough to interrupt his study.

In the scholar's opinion, the sophistication and scale of so-called cyber warfare can undoubtedly realized by one single person with one single computer, not to say many users might make spontaneous reaction to a certain event. They do not need any coordination; but the timing of the event might act as a "coordinator". Sometimes, two separate attacks might just coincided in time, target or origin, as millions of users might be online at any moment, and that two or more users with similar interest or sentiment act simultaneously does not sound so fictional.

But media might misconnect some individual people, individual events, individual targets or individual origins with each other and create some mysteries of cyber warfare. Stories from one source read imaginative; from two sources read justified; and from three or more sources read as true as facts. Once something is labeled cyber warfare, other things can be similarly labeled as well. Then the discourse of "cyber warfare" will detect its expression in real life. Cyber warfare industry will create quite good business opportunities for interested players all across the society.

Conclusion

There has been a growing concern over cyber warfare have in recent

decades. War-oriented writer usually exploited such serious and expensive terms as cyber war, information war, and electronic war to spread their impetuous and cheap ideas. More and more parties are involved in spreading the discourse about the potential threat of cyber warfare. All of them seem to benefit from an enlarged version of an imagination. A new industry is growing up, exploiting new terminologies such as cyber warfare, electronic war, and information warfare. Examples given in this essay are only tip of the iceberg. Here, I want to borrow from Morozov (2009b), saying that,

"The age of cyber-warfare has arrived. That, at any rate, is the message we are now hearing from a broad range of journalists, policy analysts, and government officials."

References

1. Derene, Glenn. How Vulnerable is U.S. Infrastructure to a Major Cyber Attack? Popular Mechanics, April 2009.
2. Economist. 2007. Cyberwarfare Is Becoming Scarier, May 24.
3. Eriksson, E. Anders. 1999. The Non-proliferation Review, Spring-Summer, pp. 57-64.
4. Gardham, Duncan. 2009. Al-Qaeda, China and Russia 'pose cyber war threat to Britain', warns Lord West, June 25, 2009. Retrieved July 17, 2009, from http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/5634820/Al-Qaeda-China-and-Russia-pose-cyber-war-threat-to-Britain-warns-Lord-West.html

5. Morozov, Evgeny. 2009a. 10 Easy Steps to Writing the Scariest Cyber Warfare Article Ever, April 11, 2009. Retrieved July 17, 2009 from http://neteffect.foreignpolicy.com/posts/2009/04/11/writing_the_scariest_article_about_cyberwarfare_in_10_easy_steps
6. Morozov, Evgeny. 2009b. Cyber-Scare: The Exaggerated Fears over Digital Warfare. Boston Review, July/August 2009.
7. Poulsen, Kevin. 2007. Estonia "Cyberwar" Wasn't. Retrieved July 17, 2009, from http://www.wired.com/threatlevel/2007/06/estonia_cyberwa/
8. Ranum, Marcus J. The Problem with Cyber War (Video), DojoSec Monthly Briefings, March 2009. Retrieved July 17, 2009, from http://securitytube.net/Cyber-War-is-Bullshit-(Dojosec)-video.aspx
9. Smith, George. 2003. Iraqi Cyberwar: an Ageless Joke. Retrieved July 17, 2009, from http://www.securityfocus.com/columnists/147
10. Smith, George. 2007. The Clowns of Cyberwar: Rediscovering electronic Pearl Harbor, always handy fodder for the lazy opinion page editor, October 8, 2007. Retrieved July 17, 2009, from http://www.dickdestiny.com/blog/2007/10/clowns-of-cyberwar-rediscovering.html
11. UK Office of Cyber Security and UK Cyber Security Operation Centre. 2009. Cyber Security Strategy of the United Kingdom, safety, security and resilience in cyber space, June 2009.

CHAPTER IX SPYWARE AND SPY AFFAIR

Spyware: a security issue, not a definition issue

The development of information and communications technology (ICTs) brings about broad survival space for both individual and organizational users. Electronic life becomes usual practice, with indicators such as growth of the number of personal computers and Internet users, the increase in the number of web sites, Internet hosts and web pages, bandwidth growth, the growth of scale of e-commerce and e-governance (Li 2008, pp. 82-89). People connected through information system might neither necessarily be as good as within a Weberian formally rational regime, nor necessarily be as bad as in a Hobbesian "war of all against all", nor as ideal as Platonian *Republic*, and Moresian *Utopia* (Li 2006d). Cybersecurity can only be perceived as a relative concept (Li 2006a; Li 2006b). Vulnerabilities of the information society loom, however, on the horizon of people's longing for an optimistic future (Li 2008, pp. 89-111). Netizens are surprised at the rise of threats of malicious codes to information security of states, enterprises and individuals, for instance. As far as cyberinsecurity and cybercrime are concerned, people have puzzled their brains to find workable solutions (see Li 1992; Li 1994; Li 2006a; Li

2006b; Li 2006c; Li 2006d; Li 2006e; Li 2007a; Li 2007b; Li 2008). Yet these ghost trouble and unwanted perplexities do not show any mercy for anyone who connected to the globalized digital networks.

One such example is spyware, which is a growing threat to the privacy of Internet users and is attracting increasing attention worldwide (Federal Trade Commission 2005; Anti-Spyware Coalition 2007; Organization for Economic Co-operation and Development 2006; Rotenberg 2008; Hackworth 2005; Saroiu, Gribble, and Levy 2004; Commission of the European Communities 2006). Spyware is a rising vexation to organizations interested in safeguarding their own proprietary intellectual property and sensitive information. It was estimated that overall malicious codes phlebotomized about 11 billion Euros from the global economy in 2005 (Computer Economics: the 2005 Malware Report, cited in Commission of the European Communities 2006, p. 3). While malware economy has ripened, one of the central obstacles that legislature is encountering when they introduce new law is still on the starting point of giving acceptable definitions (Fox 2005, pp. 1-2).

The originality of spyware has generally been traced back to online commercial advertising practice, which primarily took forms of banner and pop-up windows and was cost-ineffective. While dissemination of software with advertising functions plays an effective role in marketing, technical development promotes the evolution of spyware and increasingly spreads ActiveX controls with such functions. Creating and spreading ActiveX controls thus becomes a paid employment. Due to lack of legal foundation for making judgment concerning the nature of spreading or prohibiting spyware, developers of spyware and anti-spyware are involved themselves in circular legal actions to maintain their own interests.

Besides some kinds of spyware with clear purpose for stealing users' information, it is complicated to evaluate whether other kinds of spyware

with commercial purposes are harmful to users. Examples include assistant Internet tools, which at the same time of providing users with convenience, collect users' information. Existing laws in the world have not clearly defined them. Left undeterred, spyware continues to present substantial harms to Internet users and to the Internet as a whole (Edelman 2008).

Although there can hardly be a consensus on how to define spyware due to diversified viewpoint, to the greatest extent of proximity, it is usually regarded as installed without permission, and gathering sensitive information (sample definitions, see Anti-Spyware Coalition 2007, p. 1; Federal Trade Commission 2005, pp. 3-5; Curtin 2004, p. 1; Nelson and Simek 2006; Fox 2005, p. 2; Figliola 2006, pp. 1-3; Hackworth 2005, p. 2; Saroiu, Gribble, and Levy 2004, p. 1; Commission of the European Communities 2006, p. 3). Spyware can be used to deceive the user, forcibly revise system setup, and secretly collect information from the host computer. As a consequence of spyware infections, the victim may be inundated by pop-up advertisements, the victim's financial information or passwords may be stolen, and the victim's computer may be rendered useless. In other words, spyware can spy: capturing keystrokes, screenshots, authentication credentials, personal email addresses, web form data, internet usage habits, and other personal information, by delivering data to online attackers who use it to carry out further offences, such as identity theft, fraud, spam and so forth (Hackworth 2005, p. 2). As most misbehavior does in the cyberspace (see Li 2007b), activities involving spyware are by and large intertwined with other kinds of activities, causing far greater imperilment than it does alone.

This Chapter will put spyware on a platform of social legal phenomena, giving a review of taxonomy, characteristics, threatened interests and interest groups revolving around the standpoints for and

against the prohibition of spyware. Upon its appearances, the Chapter takes a look at current legal actions against spyware.

Spyware for spy affairs

Large and increasing is the number of spyware, the classification of which seems unmanageable and complicated. Spython (at http://www.spython.com/spyware.aspx) could detect 912 spyware programs, Paul Collins (2008) found 16,820 on the Internet, and Spyware Vaccine (at http://www.spywareremover.org/) could detect more than 50,000. Pop-Up Sentry (at http://www.popupsentry.com/spyware.html) blocked and removed 1,500 applications that are responsible for serving pop-ups. In the meanwhile, spyware can be categorized under different definitions and according to different standards. Scholars have suggested numerous plans for classifying spyware. Spywaredb (at http://www.spywaredb.com/) listed 27,604 spyware programs and identified three most common forms: adware, Trojans and cookies. Spam-site (at http://www.spam-site.com/spyware/spywaretypes.shtml) concluded spyware into four type: adware, browser hijack, keyboard logger, and modem hijacker. Software Tips and Tricks (at http://www.softwaretipsandtricks.com/windowsxp/articles/590/1/Different-types-of--Spyware) listed six types of spyware: parasiteware, adware, spyware, malware, pagehijackers, and dialers. Anti Spyware Review (at http://anti-spyware-review.toptenreviews.com/types-of-spyware.html) listed eight types: Internet URL loggers and screen recorders, chat loggers and email recorders, keyloggers and password recorders, web bugs, modem hijacking, PC hijacking, and Trojans and viruses. Free Spyware

Removal (at http://www.freespywareremoval.org/spyware-types/) grouped into six types: URL loggers and screen capture, email and chat loggers, password loggers and keystroke capture, hijacking, modem, and pop-ups. Pareto Logic (at http://www.paretologic.com/resources/types_of_spyware.aspx) listed 15 types: adware, browser helper object, browser hijacker, dialer, downloader, exploit, flooder, keylogger, malware, remote administration tool, spyware and surveillance, trackware and data miner, Trojan and worm. Consumer Software Working Group identified three practices involving the use or distribution of spyware: hijacking, surreptitious surveillance, and inhibiting termination. Boldt, Carlsson and Jacobsson (2004) grouped spyware into cookies and web bugs, adware, tracks, browser hijackers, spybots, system monitors, and malware (pp. 3-4). "iolo Technologies" (2007b) classified it into adware, browser helper object, dialer, keystroke logger, malware, remote administration and miscellaneous category.

Some other actors classify spyware without an unambiguous definition. A significant example is that of Anti-Spyware Coalition, which turns to the underlying technology, classifying spyware into eight different categories (Anti-Spyware Coalition 2007, pp. 4-5). Their classification is relatively comprehensive and broad, but blends spyware programs with both legal and illegal intentions.

Generally, four types of spyware can be identified according the two factors that should be contained in the spyware definition: secretly installed and compromising data. The first type is adware, which is designed for advertising bypassing the normal operation that the user expects. The second type is machine hijackware, which is designed for remote access or control of machine. The third type is system hijackware, which is designed to modify system and change user experience. The last type is trackware, which is designed to monitor user behavior or collect

user information. From these categories and their functions, we can intelligibly realize that not all of them are solely created for malicious intentions. Some of them were initially invented from a malicious starting point, but are later also used in legitimate marketing and managing activities. Yet some of them were first compiled for legitimate use, but are later misused. When we consider legal regulation on this issue, however, we put stress weight on the negative aspects of spyware, even though we do not necessarily view all the types and kinds as maliciously created and/or operated.

Spyware and spy ways

Spyware is located in a grey area between legal commercial software and computer viruses. Intense disagreement over the definition and classification of spyware leads to a lack of action (Braff 2005). However, the common natures of spyware are that such software is disseminated through advertisements and other social engineering means and installed forcibly or secretly on users' computers without users' knowledge or consent. Compared with software, it can have broad influence on machines and data, for example, slowing computers down, making browser display abnormal, or even despairing the systems. Its acatalapticness and uncontrollability is perceptible. Most kinds of spyware are characterized by the following three aspects:

1. Unauthorized installation. Oftentimes, adware vendors claim that their software is installed on users' computers only after users receive the agreement (Edelman 2008). Spyware typically installs itself furtively through one of three methods. Some of them are installed automatically

without the knowledge or consent of users, sometimes through bundling, that is, along with a program that the user intentionally downloads. Flourishing Peer-to-Peer file sharing software has provided good opportunities for those distributing spyware via bundling.

Users are deceived into installing spyware onto their systems because spyware authors and distributors use various social engineering techniques to induce users to install their spyware. Some are installed through deceptive means without obvious prompt. In some other cases, the computer user is asked to click “yes” or “no” to some prompt in a pop-up window, where either choice results in the installation of spyware on the user’s computer. While some spyware tricks users into installing, other spyware spreads by exploiting loopholes in applications (United States Government Accountability Office 2005, pp. 32-33), as in FTC v. Seismic Entertainment (Federal Trade Comm'n v. Seismic Entertainment Productions, Inc., Civ. No. 04-377-JD, 441 F.Supp.2d 349, 2006-1 Trade Cases ¶75,333 (D.N.H. 2006)). Users are usually more likely to get arrested by spyware when they visit adult sites, download computer programs, play online games, download music, share files, download computer games, download screensavers, and buy a product online (Fox 2005, p. 4).

2. Spyware is difficult to detect and delete by users. Spyware works in a clandestine and an obstinate way, having high capacity for self-protection. The removal of spyware is regarded as an additional difficulty (United States Government Accountability Office 2005, p. 33).

3. Disturbing normal use. Spyware can reduce functions of the computer, slowing systems down. Such disturbances may take the form of new toolbar, new desktop shortcuts, undesired homepage, unknown search engine and search results, non-default error page, repeated popup advertisements, consumption of network efficiency, jamming of network

flow, modification and deletion of data, modification of account ID and passwords, and loss of complete control over the computer. As Edelman (2008) pointed out that “a computer with spyware or adware is often virtually crippled- filled with so many popups that doing other work is impossible or impractical, and slowed so dramatically that it is unappealing to use the computer for ordinary purposes.” As a consequence, Fox (2005) estimated that millions of computers had been becoming overwhelmed with unwanted software programs that slowed performance (p. 1).

Furthermore, the prevalence of spyware affects users' online behavior as an emergency reaction. They may tend to adopt such defense mechanisms as stopping visiting particular Web sites, stopping downloading software from the Internet, stopping downloading music or video files from peer-to-peer networks, and starting using a different web browser (Fox 2005, p. 5).

4. Spying for control, and spying for confidentiality. Overall, spyware is either created for control or operated for control, compromising machine, system, or information. In detail, the working mechanisms of spyware include control over others' computers, making changes to settings or files, degrading computer operation and worker productivity, compromising information security, and posing serious security risks.

Spyware as a business

The traditional notion of spy has multifaceted meanings. Spies can always be classified into positive spies, neutral spies and negative spies, based on their roles for or against classifier's interests according to classifier's

judgment. Undoubtedly, spy being good or bad are dependent on who spies and for whom the spy spies.

With spyware's purpose for develop and target for operation, spyware can be regarded as having been developed as a new business. Unlike original types of malicious software that was created solely for the purpose of destroying users' hardware, software, or data, subsequent variants of malicious software have increasingly meddled in users' control over their own machines and data. When new variants evolved from their malicious software ancestors, they nurtured the new ambition for seeking profits. Many different players are participating in the division of labor and share of profits in this business. These players can be divided into two categories: insiders and outsiders.

Inside players are those who make a profit on or take a loss from being positively or passively involved in spyware-related activities. They can further be divided into three subcategories:

A. Symbiotic inside player: producer, beneficiary, and victimized target user. Core players in spyware industry are they, whose activities are necessary components in the industry, and without whom the emergence, existence and development of the industry would be impossible.

B. Autoecious inside player: victimized target user protector. They are those who claim to be representatives of consumers and other users. Their just existence has been dependent on the reality that consumer rights are frequently infringed.

C. Successive inside player: anti-spyware industry, security expert, legislator, law enforcement. They are those who seek overall solutions against spyware. Nevertheless, their opportunities rely on the emergence and existence of negative influence of spyware.

Outside players are those who make use of the existence of the reality

of spyware-related activities. They can further be divided into three subcategories as well:

A. Symbiotic outside player: non-beneficiary and non-victim observer. They those who are indifferent to the occurrence of spyware phenomena and the actualization of spying.

B. Autoecious outside player: mass media. They are those who claim to disclose actual facts behind the phenomena of spyware. Yet they do not take strict scientific approaches in their investigation.

C. Successive outside player: researcher and teacher. They are those who describe the phenomena, reveal the reality, explore the impact, explain the discovery, discuss different ideas, reason the hypothesis, and establish a theoretical frame.

These players have different attitude towards the creation, dissemination, operation, mischief, and general prevalence of spyware: many of them can benefit from the just negative effect of spyware on users, networks, and society (see Table 21).

Table 20 Attitude of Involved Players in Spyware Business

	Spyware tolerance	Spyware neutral	Spyware averse
Creator	Sense of achievement, financial gain, earning a high reputation		
Customer	Exploiting the function of		

	spyware to advertise, spy and attack opponent		
Target user	Fulfilling customization, getting advertised, etc.	Nothing special happens, enjoying some small annoyances	Being exploited of time, concentration, energy, and psychic. Hardware being slowed down, network being disconnected, personal information being stolen
Intruder	Easy to control others		
Real spy	Easy to spy others		
Advertiser	Easy to inform others of its products or services		
Hardware manufacturer	Encouraged to invent securer and faster machine, and new and good		

	machine makes more money. If Microsoft Windows Vista can run on an Intel Pentium 100 machine, then many current computer companies will bankrupt.		
Hardware vendor			Old types of machine may be excluded by slowing-down brought about by spyware. Hardware vendor may have a little bit to lose.
Updated hardware vendor	New type of hardware has broader market		
Software writer	Encouraged to write more secure software		
Software vendor			Old software may be disqualified in the new security

			environment. Anyway, software vendor has little to lose.
Updated software vendor	New software has broader market		
Anti-spyware producer	Winning market through panic created by spyware's broad spread. Whenever there is spyware and other viruses, there is a market for anti-virus producer. All viruses of bad nature are welcome. If you don't scare users, then we will be dismissed.		
Security expert	Current experts enjoy higher reputation and status, and get more employment opportunities		Current security expert may feel too busy dealing with security problems, and have to learn more

			sophisticated skills.
Mass media	Job opportunities, and new headlines		
Legislator	Job opportunities		
Law enforcement	Job opportunities, and new reason for budget		More work load, and new skill requirement
Professor	New field of academic career		
Researcher	New field of academic career, project and new funding opportunities		

Cerebration of international and domestic legal actions against spyware

When I dealt with the problem of general phenomena of cybercrime and explain why cyberized society created an uncontrollable situation, and explored the disputability of online content and activities, I pointed out that,

"The old and new diversity between cultures, societies and laws has not necessarily been diminished by the common networks of information systems. On the contrary, universal information systems bring in a diversity from offline to online, and bring about a diversity between offline and online." (Li 2008, p. 96) Information systems can accommodate contents of different value-orientation and activities of a differing legal nature, usually creating controversies among the various jurisdictions. As a result, the authorities in the country where the content or activities are legal cannot provide sufficient protection for people who publicize legitimate speech or carry out legitimate activities, and cannot prohibit infringements and impose sanctions on people who infringe these legal rights. Similarly, authorities in a country where the contents or activities are illegal cannot impose sanctions on people who breach the proscription, and cannot protect people who obstruct the illegal contents or activities from wrong prosecution by a country where people adopt contrary standpoints to the legal nature of these contents or activities (Li 2008, p. 99).

This diversity created a legal gap between countries of different cultural tradition, social systems and value judgment. Subsequently, countries are divided into different jurisdictions over the issue of spyware. Laws are different, and jurisdictions are different, too. Negotiations must be carried out, and consensus must be reached, both of which are unimaginably time-consuming. Appeal to international harmonization sounds like an ideal solution but impractically far-off. International harmonization has hitherto been primarily the forum of the developed countries. The working mechanism of an effective international treaty is for all of the signatory countries to take effective action and preserve a common theatre of operation. The treaty is not aimed at any third party and thus the third party is not restrained by it. Along with the

development of the Internet globally, the number of cybercrimes will be correlated with the population base of Internet penetration, and the global population base. Most of the present international harmonization measures against cybercrime have not been incorporating the countries with the largest population. This will make the measures less effective (Li 2008, pp. 334-335).

At the same time, countries may hold different attitudes towards introducing new laws against spyware. Some countries may think they have already had enough cybercrime laws tackling this issue, punishing spyware with provisions on illegal access, illegal interception, data interference, system interference, and misuse of devices as may be the case of most member states European Convention on Cybercrime. Other countries may not be possible to apply their existing laws because of their fussy process of legislation as is the case of the US. These two groups of countries cannot simply reach a consensus on applying existing international agreements.

Then we have to sue to domestic law. Domestic law is much easier to be enacted than an international treaty. Within a country, however, the above-mentioned diversity can well be translated into the field of conflict of interests. Today, it is straightforward to recognize that feasible domestic legislation and enforcement can assist to prevent the negative influence of spyware (Edelman 2008). However, legislation and enforcement are not an issue of whether there exist an unambiguous definition on what are malicious spyware and whether malicious spyware should be prohibited, but an issue of tussle between interest groups and their representatives in legislature and judicial organs. Anti-spyware advocators believe that current legal actions are inadequate, while opponents argue that industry self-regulation and enforcement of existing laws are sufficient (Figliola 2006, p. 1). Disputation occurs whenever

confront the spyware creators; disseminators; advertisers; consumers; state, business and personal secret keepers; privacy protectors; legislators of various value-orientation; and law enforcers of different interest. In a word, there can not be a single discourse concerning whom the law will protect and prohibit. Law's goals can become promiscuous and bedimmed if no law at all. Legislative practice in the US against spyware has already taught us plenteous lessons (see a random example in Wenham 2002).

In the US, as of September 2008, no federal has been enacted specifically against spyware. Different pieces of anti-spyware legislation have passed the House of Representatives but have not proceeded any further. At the state level, as of March 2008, fourteen state legislatures have adopted some form of anti-spyware legislation and more states are considering anti-spyware legislation. Indeed, some states have computer trespass or computer privacy statutes that effectively prohibit the use of spyware. Spyware legislation has been passed in Alaska (Alaska Stat. §45.45.792), Arizona (Ariz. Rev. Stat. Ann. §§44-7301 to 44-7304), Arkansas (Ark. Stat. Ann. §§4-11-101 to 4-11-105, Ark. Stat. Ann. §19-6-301, Ark. Stat. Ann. §19-6-804), California (Cal. Bus. & Prof. Code D. 8 §§22947 to 22947.6), Georgia (Ga. Code §§16-9-152, 16-9-157), Indiana (Ind. Code §24-4.8-1 et seq., Ind. Code §24-4.8-2 et seq, Ind. Code §24-4.8-3 et seq.), Iowa (Iowa Code §§715.1 to 715.8), Louisiana (La. Rev. Stat. Ann. §§51:2006 to 51:2018), Nevada (Nev. Rev. Stat. §205.4737), New Hampshire (N.H. Rev. Stat. Ann. §§359-H:1 to 359-H:6), Rhode Island (R.I. Gen. Laws §11-52.2-2, R.I. Gen. Laws §11-52.2-7), Texas (Tex. Business & Commerce Code Ann. §§48.001 to 48.203, Tex. Business & Commerce Code Ann. §§324.001 to 324.102), Utah (Utah Code Ann. §§13-40-101 to 13-40-401), and Washington (Wash. Rev. Code §§19.270.101 to 19.270.900) (National Conference of State Legislatures. 2008). They represent 28 percent of the U.S. states. Having new laws is one of the many alternative

solutions for this new issue.

In recent years, however, dozens of cases have also been filed against spyware. At least 11 actions have been taken by FTC. Others have been taken at state and federal levels. The prohibited activities in these cases can fall into one or more of the following:

1. Tracking consumers' Internet activity or collects other personal intonation;

2. Changing consumers' preferred Internet homepage or other browser settings;

3. Inserting a new toolbar onto consumers' Internet browsers, inserts a new bar, frame or window onto consumers' browser windows that in turn displays advertisements;

4. Displaying numerous "pop up" advertisements on consumers' computer screens during a single computer session, even when consumers' Internet browsers are closed;

5. Installing a dialer program on consumers' computers;

6. Changing a user s "error" page or DNS page;

7. Inserting advertising hyperlinks into third-party webpages; or

8. Installing other advertising software code, file, or content on consumers' computers (see FTC v. ERG Ventures, LLC, Civil Action No.: 3:06-CV-00578-LRH-VPC, FTC File Nos.: 062-3192; X070004; FTC v. Enternet Media, Inc. Conspy and Co, Inc. Lida Rohbani, Nima Hakimi, Baback Hakimi and Nicholas C. Albert, Civil Action No.: CV05-7777CAS (AJWx), FTC File No.: 052 3135; FTC File No. X06-0003).

From these cases, we can see that existing laws, either those not specifically designed against spyware or those specifically designed against spyware, have been applied in legal fight against spyware. A

diversified range of provisions on offences can be applied to the acts involving spyware, including, for example,

1. Knowingly and with intent to defraud trafficking in or using one or more unauthorized access devices during any one-year period, and by such conduct obtaining anything of value aggregating $1,000 or more during that period (U.S.C.§1029(a)(2)) (United States v. Mario Alberto Simbaqueba Bonilla).

2. Intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information from any department or agency of the United States (18 U.S.C. §1030(a) (2) (B) (United States v. Kenneth Kwak).

3. Intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information from any protected computer if the conduct involved an interstate or foreign communication (18 U.S.C. §1030(a) (2) (C)) (United States v. George Nkansah Owusu; United States v. John J. Gannitto; United States v. Cheryl Ann Young).

4. Knowingly and with intent to defraud, accessing a protected computer without authorization, or exceeding authorized access, and by means of such conduct furthering the intended fraud and obtaining anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period (18 U.S.C. §1030(a) (4)) (United States Hario Tandiwidjojo; United States v. John Schiefer; United States v. Van T. Dinh; United States v. Juju Jiang).

5. Knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer (18 U.S.C

§1030(a)(5)(A)(i))(United States v. Christopher Maxwell; United States v. Jeanson James Ancheta; United States v. Robert Matthew Bentley; United States v. Jason Michael Downey).

6. Causing (or, in the case of an attempted offense, would, if completed, have caused) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value (18 U.S.C.§1030(a)(5)(B)(i)) (United States v. Christopher Maxwell; United States v. Robert Matthew Bentley).

7. Causing the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals (18 U.S.C. §1030(a) (5) (B) (ii)) (United States v. Christopher Maxwell).

8. Causing damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security (18 U.S.C. §1030(a) (5) (B) (v)) (United States v. Kenneth Kwak).

9. Intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication (18 U.S.C.§2511(1)(a)) (United States v. Jerome T. Heckenkamp; United States v. Cheryl Ann Young).

10. Sending through the mail, or sending or carrying in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications (18 U.S.C. §2512(1)(a))(United States v. Carlos Enrique Perez-Melara).

11. Manufacturing, assembling, possessing, or selling any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce (18 U.S.C. §2512(1) (b)) (United States v. Carlos Enrique Perez-Melara).

12. Placing in any newspaper, magazine, handbill, or other publication or disseminating by electronic means any advertisement of any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications (18 U.S.C. §2512(1)(c)(i)), or any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications, knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce (18 U.S.C. §2512(1)(c)(ii)) (United States v. Carlos Enrique Perez-Melara).

Some other cases fall into unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce (15 U.S.C. §§45(a) (b)) (FTC v. ERG Ventures, LLC).

Indeed, these clauses and cases have been effective in establishing a certain degree of deterrence against malicious profit-harvesters in spyware business. It is not impossible that existing laws can be applied to phenomena with a bit new features. The options have to be weighed against the price of legislating process. In Europe, it is more likely that the current Convention on Cybercrime will be applied to the issue of spyware, when an act causes comparable harm as that of illegal access,

illegal interception, data interference, system interference, and misuse of devices. The advantage of a broadly defined consensus in advance can be perceived if legislators in the world cannot follow the change of technologies, unless legislators are powerful enough, as in the US, to obtain inexhaustible budget for their lobbying in endless legislating activities.

Conclusion

Spyware poses a substantial menace to security, integrity and confidentiality of information systems. Originating from online commercial advertising strategies, spyware can be used to deceive users, forcibly revise system setup, and secretly collect information from host computer. This Chapter puts spyware on a platform of social legal phenomena, giving a review of taxonomy, characteristics, threatened interests and interest group revolving around the standpoints for and against the prohibition of spyware. Spyware is developing as a new business. Many different players are participating in the division of labor and share of profits in this business. These players can be divided into insiders and outsiders. Upon its appearances, the Chapter takes a look at current legal actions against spyware. Even though there have been abundant reasons to be sure that old laws are not sufficient to prevent spyware in general, to some extent, existing laws provide effective means for combating some specific spyware-related activities.

References

1. Anti-Spyware Coalition, 2007.Anti-Spyware Coalition Definitions and Supporting Documents, Working Report, October 27.

2. Boldt, M., Carlsson, B. and Jacobsson, A. 2004. Exploring Spyware Effects, in proceedings of Nordsec 2004, Helsinki.

3. Braff, Andrew T. 2005. Defining Spyware: Necessary or Dangerous, Shidler Journal of Law, Commerce and Technology, Volume 2, Issue 1. Retrieved September 20, 2008, from http://www.lctjournal.washington.edu/Vol2/a001Braff.html

4. Collins, Paul. 2008. Startup Programs and Excutables Listing. Retrieved September 20, 2008, from http://www.lafn.org/webconnect/mentor/startup/PENINDEX.HTM.

5. Commission of the European Communities. 2006. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: On Fighting Spam, Spyware and Malicious Software COM (2006)688 final, Brussels, November 15.

6. Consumer Software Working Group. 2004. Examples of Unfair, Deceptive or Devious Practices Involving Software. Retrieved September 20, 2008, from http://www.cdt.org/privacy/spyware/20040419cswg.pdf

7. Curtin, C. M. 2004. Spying on Spyware, Interhack Proprietary: Public/5/5.

8. Edelman, Benjamin. 2008. Testimony of Benjamin Edelman before the United States Senate Committee on Commerce, Science and Transportation, June 11.

9. Federal Trade Commission. 2005. Spyware Workshop: Monitoring Software On Your Personal Computer: Spyware, Adware, and Other Software: Report of the Federal Trade Commission Staff, Diane Publishing.

10. Figliola, P. M. 2006. Spyware: Background and Policy Issues for Congress, July 17.

11. Fox, Susannah. 2005. Spyware: The Threat of Unwanted Software Programs Is Changing the Way People Use the Internet, Pew Internet & American Life Project.

12. Hacvkworth, Aaron. 2005. Spyware, CERT Coordination Center,Carnegie Mellon University.

13. Iolo Technologies, LLC. 2007a. List of spyware supported by Spython™ . Retrieved September 20, 2008, from http://www.spython.com/spyware.aspx

14. Iolo Technologies, LLC. 2007b. Spyware Categories. Retrieved September 20, 2008, from http://www.spython.com/categories.aspx

15. Li, Xingan. 1992. Jisuanji Fanzui Xingfa Shiyong Wenti Chutan (Exploration into Issues of Application of Criminal Law to Computer Crime), Yanjisheng faxue (Graduate Law Review), Issue 3 (in Chinese).

16. Li, Xingan. 1994. Jisuanji Fanzui Ruogan Wenti zhi Yanjiu (A Study on Several Issues in Computer Crime), China University of Political Science and Law, Beijing: China University of Political Science and Law, Master's degree thesis (in Chinese).

17. Li, Xingan. 2006a. Economic Analysis of Cybersecurity: The Mixed Provision of Private Good, in John Roufagalas, ed. Resource Allocation and Institutions: Exploring in Economics, Finance and

Law, Athens, Greece: ATINER, pp. 607-620.

18. Li, Xingan. 2006b. Relative Concept of Cybersecurity, Information and Security: An International Journal, Volume 18, pp. 11-24.

19. Li, Xingan. 2006c. E-marketing, Unsolicited Commercial E-mail, and Legal Solutions, Webology, Volume 3, Number 1. Retrieved September 20, 2008, from http://www.webology.ir/2006/v3n1/a23.html

20. Li, Xingan. 2006d. Cyberspace and the Informed Rationality of Law, in Ahti Laitinen ed. Writings in the Sociology of Law and Criminology, University of Turku Faculty of Law.

21. Li, Xingan. 2006e. The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited through Typical Cases Prosecuted, University of Ottawa Law and Technology Journal (accepted in 2006, in press).

22. Li, Xingan. 2007a. International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene, Webology, Volume 4, Number 3. Retrieved September 20, 2008, from http://www.webology.ir/2007/v4n3/a45.html

23. Li, Xingan. 2007b. The Phenomenon of Unsolicited E-mails with Attachments, SIMILE: Studies In Media and Information Literacy Education, Volume 7, Number 2, May 2007, DOI 10.3138/sim.7.2.003, pp. 1-11.

24. Li, Xingan. 2008. Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society, Turku, Finland: Uniprint.

25. National Conference of State Legislatures. 2008. State Laws Regarding Spyware. Retrieved September 20, 2008, from

http://www.ncsl.org/programs/lis/privacy/spywarelaws.htm

26. Nelson, Sharon D. and Simek, John. 2006. Muddy Waters: Spyware's Legal and Ethical Implications, GPSolo Magazine, ABA General Practice, Solo & Small Firm Division (Jan./Feb.)

27. Organisation for Economic Co-operation and Development. 2006. Report of the OECD Task Force on Spam: Anti-Spam Toolkit of Recommended Policies and Measures, DSTI/CP/ICCP/SPAM(2005)3/FINAL, August 19.

28. Rotenberg, Marc. 2008. Testimony and Statement for the Record of Marc Rotenberg: Hearing on "Impact and Policy Implications of Spyware on Consumers and Businesses" Before the United States Senate Committee on Commerce, Science and Transportation, June 11, Washington, DC.

29. Saroiu, S., Gribble, S. D., and Levy, H. M. 2004. Measurement and Analysis of Spyware in a University Environment, Proceedings of the 1st conference on Symposium on Networked Systems Design and Implementation - Volume 1, San Francisco, California.

30. United States Government Accountability Office. 2005. Report to Congressional Requesters-Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems.

31. Wenham, C. 2002. A Law to Protect Spyware, April 26. Retrieved September 20, 2008, from http://dir.salon.com/story/tech/feature/2002/04/26/hollings_spyware/index.html

32. Zhang, Yulin. 2006. Liumang Ruanjian: Youzou zai Falv de Bianyuan (Malicious Software: Wandering between Law's Margins), Zhongguo Jisuanji Yonghu (China Computer Users), Issue 37, 2006 (in Chinese).

CHAPTER X ECONOMIC APPROACH TO CYBERCRIME

General theory of punishment in law and economics

The idea of deterrence has existed in fragmented forms for several centuries in both eastern and western philosophy and law.[6] However, it is generally accepted that the identification of economic aspects in illegal activities began in the US in the late 1960s. Gary S. Becker's article "Crime and Punishment: An Economic Approach", published in 1968, is considered the earliest study of crime from an economic perspective. Becker seeks to observe criminal behaviour in the light of purely economic factors as he perceives crime as the consequence of rational estimations of the lawbreaker. The economic approach to crime starts from a plain hypothesis that all people take action rationally, and make a decision whether to perpetrate crime by comparing the benefits and costs of engaging in crime. If the action produces more expected benefits than expected costs, the person will carry out the action, even if it is an unlawful act.

[6] The literature presenting the deterrence argument goes back to Beccaria (1774); Bentham (1789); and Blackstone (1765–69).

The individual estimates all her or his actual opportunities of gaining legal returns, the sum of returns offered by these opportunities, the sum of returns offered by different illicit ways, the probability of being arrested if she or he acts illegally, and the possible penalty if she or he is seized. After making these estimations, she or he chooses the act or profession with the maximum discounted return.[7]

The two fundamental points of departure can be summarized as:

Crime rates respond to the costs and benefits of committing crime;

People respond to deterring incentives.

It followings that devoting resources to detection, conviction and punishment should influence the level of crime. The deterrence hypothesis can be illustrated by Figure 1. The horizontal axis shows the amount of crime committed by an individual, which could be measured by the number of offences and the vertical axis measures costs and benefits. If the marginal cost (MC_1) of criminal activity rise and the marginal benefits (MB) fall, as shown, there is an optimal level of crime (C*) where marginal cost intersects marginal benefit. Marginal cost shows the minimum return required before an individual would engage in successive units of crimes: it is therefore a supply function for crime. Marginal benefit shows the maximum the individual would pay for the opportunity to undertake successive units of crime, ignoring his costs, and can be regarded as the demand for crime.

Economists suggests we can influence individuals to reduce their criminal activity by undertaking policies to shift the marginal cost function upwards and the marginal benefit function downwards.

Following Becker (1968), the deterrence hypothesis can be formulated as:

---

[7] Becker as cited in Sullivan (1973), p.141.

$EU=pU(Y-f)+(1-p)U(Y)$

Where p=probability of capture and punishment; U=utility (assumed measurable); EU=expected utility; f=value of punishment; Y=income if undetected. The cost-benefit calculation of the rational criminal implies that both increasing the probability of detection and increasing the severity of the punishment reduce the criminal's expected utility and should deter crime.

An extensive scope of economic studies of crime has been undertaken since Becker's preliminary work.[8] To date, the application of these theoretical frameworks has been established on or expanded to the field of particular crimes. During this process, the classic theories have been undergoing continuous revision and updating.

At the same time, the crimes people commit changes as the society changes. It has already been recognized that with the advent of complex computer technology, social changes brought about by technology appear capable of occurring with devastating rapidity. The social scientists must try to recognize the bases of change more quickly in the information age[9] than before (Peters 1971:31). While the economy is increasingly dependent on the information systems, the cybercrime is eroding the basis of this economy. How to implement suitable punishment to cybercrime? This is one of the questions law and economics must be devoted to answer. There have already been a number of initial efforts to analyze cybercrime and punishment with this approach, though the current achievements are relatively fragmented.

However, it should be always borne in mind that supremacist

[8] For example, Stigler (1970); Harris (1970); Ehrlich (1973, 1975); Ehrlich and Mark (1977). For an overview of the early literature on the economics of crime see Sullivan (1973). For more recent studies see, Adreano (1980); Findlay (1999); Hellmann (1980); Rottenberg (1973).

[9] The term "Information Age' was coined by Wilson Dizard in his 1982 book "The coming information age: an overview of technology, economics, and politics", published by Longman in New York in 1982.

viewpoint about law and economics have always been criticized in the academia. Biological, psychological, social, political, religious, and lifestyle factors have certain influences on crime. Mental illness and duress of unemployment may be the just reasons why people in the condition become irrational risk takers. Buchanan and Hartley's (1992) allegation that if criminals were genetically predisposed towards a life of crime, it would be difficult to give explanation to why the original prisoner population of Australia did not bring about a heaven of criminals, apparently ignores the fact that the biological factors do not always represent genetic factors. The deterrent mechanism does not work when we punish those who do harm to others under mental illness, or under necessity. That's why laws provide that these situations are defenses against indicting. While we more and more turn to economic analysis, we are not completely refusing the contribution of other elements in the phenomenon of crime.

Factors influencing the detection and conviction probability of cybercrime

Cybercrime is highly concealed

For the hackers, the likelihood of being caught and convicted is low. The greatest advantage to a cybercrime is the ability to commit crimes against people and never be punished or even identified (Philip 2002). There are countless cybercrimes that are not made public due to private industry's reluctance to publicize its vulnerability and the government's concern for security (Hatcher et al. 1999: 397, 399). The term "dark figure", used by

criminologists to refer to unreported crime, has been applied to undiscovered computer crimes (UN Manual, par. 30). The computer criminal is less likely to be caught than the bank robber is, and less likely to be convicted. Because of limited awareness and experience of system administrators and users, many intrusions are not detected (COM(2000) 890 final, 11).

Firstly, one of the biggest difficulties law enforcement agencies face is that electronic crimes are difficult to detect (Wolf 2000:100). The electronic records or software resulting from the offences can be electronically altered, deleted or erased by hackers in a brief instant, or in the normal course of events, before it can be captured as evidence (Park 2004; Parker and Nycum 1984:313). Untraceable use of an Internet site, with the permission of the site's controllers, is quite easy to arrange. Even if we record the intruder's activities and try to trace him to his source, this would require a long term of work and the cooperation of many organizations[10] in possibly many countries. Roughly speaking, less than one in ten successful computer intrusions are detected (Molander et al. 1996).

Secondly, it is possible for people to remain anonymous while communicating or performing other activities over the Internet. At the user level, the account's name of email messages and newsgroup articles is not required to bear any resemblance to that of its user; a considerable degree of anonymity is available. If complete anonymity is wanted, a file can be sent to another user who then retransmits it as a newsgroup article or electronic mail message. If the retransmitting user is an automatic

---

10 See generally Stoll (1988), 484-497 (telling a story of how Lawrence Berkeley Laboratory traced a German trespasser on the U. S. military networks, who slipped through operating system security holes and browsed through sensitive databases. "Tracing the activity was challenge because the intruder crossed many networks, seldom connected for more than a few minutes at a time, and might be active at any time." Ibid, 486).

program rather than a person, the protection is even greater. Evidently, such an arrangement makes identification of and enforcement of laws against the sender extremely intricate, particularly if the retransmitter is in another jurisdiction (Kingdon 1994).

Because of the make-up of the Internet, it is sometimes difficult for law enforcement officers to discover the identity of a hacker (Harris 2001). A hacker might hide or "spoof" his IP address, or might intentionally bounce his communications through many intermediate computers scattered throughout the world before arriving at a target computer. The investigator must then identify all the bounce points to find the location of the hacker, but usually can only trace the hacker back one bounce point at a time. In cases that a victim who has no record of the IP address, that some ISPs lack of the mechanisms to keep suitable records, that some computer hackers alter the logs, or that some leads go through foreign countries which do not consider hacking a crime, this limits law enforcement officers to traditional investigative techniques, which alone may be inadequate to identify the hacker (National Police Agency 1998).

At the same time, it is not difficult to introduce a new computer to the Internet that has the ability to be recognized anywhere on the Internet. Registration requirements are not difficult to satisfy, and there is little to prevent transfer of the site to new controllers. In general, proof of identity requirements for Internet use is very weak (Department of Treasury Office of Tax Policy 1996:24).

Furthermore, people are always anxious that, without anonymity on the Internet, it is not possible to guarantee fundamental rights (COM(2000) 890 final, 20; National Police Agency 1998). The European Union Data Protection Working Party’s Recommendation considers the issue of anonymity on the Internet as being at the centre of a dilemma for

governments and international organizations.[11] On the one hand, the possibility of remaining anonymous is essential if the fundamental rights to privacy and freedom of expression are to be maintained in cyberspace. On the other hand, the ability to participate and communicate online without revealing one's identity runs against the grain of initiatives being developed to support the fight against cybercrime (COM(2000) 890 final, 20). This brings a sense of security, and gives individuals the courage to do the outrageous and sometimes even resort to illegal activities (Philip 2002). Individuals may seek to play pranks, or steal, cause loss or harm, or commit fraud. It sometimes takes days, weeks or even months before acts of cybercrime are detected, and by that time the perpetrators are able to cover their tracks and maintain their anonymity (Philip 2002).

Thirdly, the mechanisms by which crimes are enacted within computers are sometimes invisible to the corporate or organisational victims (Parker and Nycum 1984:313). The invisibility of cybercrimes is based on several factors: sophisticated technology, investigating officials' lack of sufficient training, absent of victims' contingency plan for responding to incidents, and the reluctance of victims to report computer offences (UN Manual, par. 30, 31). Even if intrusions are detected, victims tend not to report intrusions, particularly to law enforcement. In cases, the victim company does not know which law enforcement entity to call (Salgado 2001). Frequently quoted sources place figures for reporting intrusions to law enforcement between 11% and 17%.[12] The documented reasons behind the reluctance to take legal actions are mainly for fear of adverse publicity, public embarrassment or loss of goodwill, the loss of investor or public confidence, the resulting economic consequences such as

11 The Article 29 Data Protection Working Party (1999).

12 See Mardesich (1996), 1E.

the panic effect that this information would create on their stock prices, [13] and exposure to future attacks (COM(2000) 890 final, 11). Some experts have suggested that these factors have a significant impact on the detection of computer crime (UN Manual, par. 31). The rate of unknown occurrences of computer crimes has increased as a result (Park 2004).

Fourthly, unlike more traditional threats that the criminal is physically present at the crime scene, the cybercriminal usually is not present at the crime scene thus making apprehension difficult (Speer 2000:260). Cybercrimes are jurisdictionally complex, usually necessitating involvement by more than one authority, and often hindering state authorities' ability to pursue complete investigations (Roush 1995:36). In an increasingly networked world, it is increasingly likely that an intruder would enter at least one foreign system, perhaps even without knowledge of having done so. Legal measures to ease these jurisdictional impediments are not unattainable, but are likely to place an even greater burden on an international response (Ramo 1996:32).

Finally, many of the technological advances that benefit businesses hinder investigative efforts (Institute for Security Technology Studies 2002). The burden imposed by jurisdictional complexities is aggravated by the highly resource-intensive nature of computer crime investigations. Staffing a response capability involves the cost of procuring and frequently updating hardware and software, and training and retaining qualified personnel. [14] Perhaps most significantly, these investigations are extraordinarily time-intensive (O'Connor 1997:3C).

---

13 See Carter (1995), 21; Roush (1995), 32, 34; Gelbstein and Kamal (2002), 2; McKenna (2003) (reporting that research carried out in December 2002 among 40 members of IISyG - a group of IT security directors and managers in the City of London and in government - revealed that fear of damage to corporate reputation prevented over two-thirds of organisations from reporting incidences of cybercrime. Companies scared of damaging their corporate image are masking the true extent of cybercrime.)

14 See generally Philip (2002).

Needs are revealed in areas such as data collection, log analysis, and Internet protocol tracing (Institute for Security Technology Studies 2004). The needs of cyber investigators have not been met by the available technology solutions (American Society for Industrial Security 2004:40). In order to fill the jobs that opened, the FBI is aggressively recruiting people with electrical engineering and computer-science backgrounds. For those applicants, it has waived its usual requirement of three years of work experience (Fields 2004).

Of course, there is inevitably critics pointing out that the cyber policemen always ask for more money, more wiretap, bugs in computers and sell phones, weak encryption and permission to implement Clipper chip technology.[15] Nevertheless, no more arrests follow (Koch 2000).

The criminal's concealment costs themselves are a social waste.[16] Concealment may also exert other costs on society. It may decrease a crime's expected sanction, and thus decrease the incentives not to cause harm to others. In addition, concealing activities on the part of criminals raise the law enforcement costs that must be spent to reach this probabilistic level.[17]

The concealment of cybercrime proves the low probability of punishment. The prosecution of cybercrime is very expensive. Only the large severity of the penalty can increase the expected cost of the

---

[15] CLIPPER is an NSA developed, hardware oriented, cryptographic device that implements a symmetric encryption/decryption algorithm and a law enforcement satisfying key escrow system. While the escrow management system design is not completely designed, the cryptographic algorithm (SKIPJACK) is completely specified (and classified SECRET). The cryptographic algorithm has the following characteristics: 1.Symmetric, 80-bit key encryption/decryption algorithm; 2. Similar in function to DES (namely, basically a 64-bit code book transformation that can be used in the same four modes of operation as specified for DES in FIPS81); 3. 2 rounds of processing per single encrypt/decrypt operation; 4. Design started by NSA in 1985; evaluation completed in 1990. See Computer Security Devision (1993).

16 That the costs of committing crimes are social wastes was noted by Tullock (1967).

[17] C.f. Stanley (1995), p.2.

cybercriminal and thus deter more cybercrime. However, with no penalty for some less serious crimes and only severe penalty for more serious crimes, there would seem to be incentives for a lot of less serious crimes. Given the same level of punishment of different level of crimes, some criminals who would have committed less serious crimes may find it worthwhile to commit crimes that are more serious.[18] This is due to that the marginal deterrence would be weaker if there is less difference between the punishments of the two types of crimes. Using more severe punishments for less serious crimes often precludes using a graduated schedule of punishments as a deterrent to more serious crimes. The more serious crimes have a greater payoff than less serious crime, but the punishment was the same. Therefore, if one were going to commit the crime, there would be a strong incentive to commit the more serious one. The schedule of punishment does not reflect the concept of marginal deterrence.[19]

Cybercrime is transnational and ubiquitous, obstructing the establishment of jurisdiction

In any country, the court must have jurisdiction over the person or the subject matter of a lawsuit in order to be able to try it. This works well with the current setup of law enforcement agencies that are very territorial and operate within distinct village, town, district, city, county, state or province, or country lines. However, unauthorised access to information systems can be accomplished from virtually anywhere on the

[18] Ibid.
[19] Ibid.

network,[20] because the communications capability of cyberspace allows criminals to more easily conspire to commit crimes, and to do so without being in geographic proximity of one another or the target (Lenk 1997). The international characteristic of cybercrime is evident (National Police Agency 1998). The area of legal jurisdiction further complicates the cybercrime enforcement (Lee et al. 1999:873). Since different countries have different laws about computer crime, questions can arise as to whether a "crime" has actually been committed at all (Lenk 1997).

Smith, Grabosky, and Urbas (2004) concluded that the transnational dimension of cybercrime poses four formidable challenges for prosecutors: to determine whether the conduct in question is criminal in their own jurisdiction, to assemble sufficient evidence to mobilise the law, to identify the perpetrator and to determine his or her location, and to decide whether to leave the matter to local authorities or extradite the offender (Smith, Grabosky and Urbas 2004:48-49). While the major international organisations, like the Organisation for Economic Cooperation and Development (OECD) and the Group of Eight, are seriously discussing cooperative schemes, many countries do not share the urgency to combat cybercrime for many reasons, including different values concerning piracy and espionage or the need to address more pressing social problems. These countries, inadvertently or not, present the cybercriminals with a safe haven to operate. Never before has it been so easy to commit a crime in one jurisdiction while hiding behind the jurisdiction of another.

The elimination of borders favours interjurisdictional criminal

---

20 See the United States v. Tenebaumv (Israel), 18 March 1998, Israeli hacked United States military computers; United States v. Gorshkov (W.D. Wash) 4 October 2002, Russian hacker; United States v. McKinnon I (E.D. Va.) and II (D. N.J.) 12 November 2002, British National hacked into United States Military Networks; United States v. Zezev (S.D. N.Y.) 1 July 2003, Hackers from Kazakhstan; United States v. Ivanov (D. Conn.) 25 July 2003, Russian hacker, also charged in C.D. Cal ,E.D. Cal , W.D. Wash. and D. N.J.

mobility. Rational criminals will commit their acts where the marginal cost of one more crime is lower (Garoupa 2003). This marginal cost is determined by law enforcement policies and transportation and communication costs. This effect should lead to competition among the different jurisdictions to have a tougher law enforcement policy in order to avoid immigration of offenders. This competition would produce a waste of resources because each jurisdiction ignores the loss of welfare on other jurisdictions. Therefore, a cooperative solution internalizes this externality (Garoupa 2003). Due to the difficulty in establishing jurisdiction, even if a certain offence is detected, it is still uncertain whether the way leads to punishment.

Suggestions have been made to incorporate cyberspace into various jurisdiction frameworks. However, this will take a great deal of time, agreement and co-operation between countries. Various countries are still struggling to establish treaties to sort out these issues.

Cybercrime is complicated, prohibiting efficient investigation, evidence collection and conviction

The Internet allows for communication and planning of criminal activity in different ways than in even the recent past.[21] To make matters worse, the information on how to infiltrate a corporation is freely available on the Internet (Behar 1997:66). The incapacities stem ultimately from the fact that the information infrastructure is transnational in nature. Attackers

21 C.f. Lenk (1997). The evolution of the attack mechanism in 1982 is password guessing, 1984 Self-replicating code, 1985 password cracking, 1986 Exploiting known vulnerabilities, 1988 Disabling audit mechanisms, 1989 Use of back doors in programs, 1990 Hijacking sessions, 1991 Sweepers, 1992 Packet sniffers, 1993 Stealth diagnostics, 1994 Packet spoofing, 1995 Graphic user interfaces for attack tools, 1996 Automated probes and scans, 1997 Denial of service, 1998 Web attacks, 1999 Macro viruses, and 2000 distributed attacks. See Longstaff (1999).

deliberately fashion their efforts to exploit the absence of internationally agreed standards of behaviour and cooperation. Attackers can avoid prosecution or greatly complicate investigations simply by initiating attack packets from countries with inadequate laws, and routing them through countries that with different laws and practices, and no structures for cooperation (Sofaer et al. 2000).

Any corporation connected to the Internet is vulnerable to hacker intrusions because the Internet is accessed by hundreds of millions of people (Adams 1996:406).

Cybercrime is expensive, attracting more potential offenders to produce it

In the sense of losses caused by cybercrime, it is so expensive that no other activity can be its substitute. Sometimes, the "losses" of an offence might not necessarily be pure social cost. Some of the wealth might be transferred from the victim to the offender. Generally, the more the offender obtains, the more the victim loses. In some other cases where the offender does not acquire substantial property, the "losses" of a victim's money or health has meaning in satisfying the offender's psychological demand. Both cases, the offender has expected benefits. Again, the more the victim loses, or the more seriously the victim is damaged, the more the offender is satisfied.

In understanding the costs of crime, the usable approach is the accounting exercise where researchers just try to add up all of the losses from crime. The largest loss category is usually the values of lives lost due to murder. Other straightforward costs include the amount that is spent on crime prevention. These costs would include the amount that is spent by the government on police and the judiciary. Crimes cost estimates have

generally been unable to quantify the social costs that accrue from underinvestment in the legal sector because criminals appropriate returns.

It has proved difficult to give an accurate, reliable overview of the extent of losses and the actual number of cybercriminal offences (UN Manual, par. 27). Serious damages can be caused by either one or just a few persons' simple operations or tricks. Especially, by taking advantage of the development of the ICT where various computer systems are connected together by online networking, a few professional hackers are capable of breaking down national infrastructures and major communication systems (Park 2004).

Notwithstanding the whole world is being acting actively to combat cybercrime, the number of cybercrime is still on the rise and that their cost is increasing exponentially (CSI/FBI 2000). International estimates indicate that cybercrime costs approximately $50 billion annually in 2002 (Hale 2002:5-6), and reached $400 billion in 2005 (McAfee Virtual Criminology Report 2005:5). The meaning of this 2005 number may be well understood if we compare it with the "911" attacks[22] which cost New York City at least $17 billion. And terrorism is forecast to knock .25% off the world economy's growth rate - an impact of around $75 billion (Davidson 2003). That is to say, the worldwide overall cybercrimes bleed the economy nearly 24 times of the "911", if they are comparable. In addition, companies are investing heavily in a variety of security

[22] The September 11, 2001 attacks were a series of coordinated attacks carried out in the United States on Tuesday, September 11, 2001. According to the official 9/11 Commission Report, nineteen men hijacked four commercial airliners. Two were crashed into the World Trade Center, shortly after which both towers collapsed. The third aircraft crashed into the the Pentagon. The fourth plane crashed into a rural field in Pennsylvania. The attacks were the most lethal terrorist acts ever carried out in the United States and most lethal individual attacks in the world. The September 11th attacks are arguably the most significant events to have occurred so far in the 21st century in terms of the profound economic, social, cultural, and military effects that followed in the United States and many parts of the world. See generally National Commission on Terrorist Attacks upon the United states, 9/11 Commission report, August 2004, at http://www.9-11commission.gov/report/911Report.pdf.

technologies. These investments are dramatic evidence of the huge costs being inflicted by cybercrime. To these amounts must be added the costs of cybercrime insurance, a new coverage for an expanding market. This is not unrealistic, if we recall that the IMF June 2002 Global Financial Stability Report reflects a conservative total insured losses for 911 of around 44 billion US Dollars (IMF 2002:38).

The direct cost typically associated with preventing or recovering from cybercrime-investments in intrusion-detention systems, lost productivity, overtime for IT staff to fix compromised systems-have all become an unfortunate but accepted part of doing business, and they rarely affect a company's revenue over time or its stock prices. The real financial damage done by cybercrime stems from breaches of confidence. Such breaches can drive down revenue over time, and stock market investors consider that possibility by lowering their estimation of the worth of the company's stock. Companies that suffer a confidentiality violation lose more than 5 percent of their market value on average (Loeb 2004:69).

A survey by Sunil Wattal and Rahul Telang of Carnegie Mellon University in Pittsburgh, Pennsylvania, analysed the economic impact on 18 software suppliers, including Microsoft, Cisco, IBM and Red Hat. Announcing vulnerability in one of these companies' products caused, on average, a 0.6 per cent fall in its stock price, or an $860 million fall in the company's value (Telang and Wattal 2005:3).

Costs of cybercrime are only a part of the social loss of cybercrime. According to Becker, the social loss of crime was defined as the sum of the costs of crime, costs of arrests and convictions, and the costs of sanctions. The probability and severity of punishment was determined in order to minimize this sum (Becker 1968). Costs of cybercrime are difficult to measure; however, these costs are reasonably substantial (Garg et al. 2003) and are essentially doubling each year (Lukasik 2000). The problem

becomes even more complicated when one considers that these crimes are underreported (Ullman and Ferrera 1998).

What makes the situation worse is that cybercrime is not only expensive, but also is in the process of rapid increase. Only if it reaches the stage of saturation, the development speed could begin to decrease. Furthermore, Public-funded law enforcement is stymied by territorial laws and frontiers that are not even lines on the map in cyberspace. Budget-constrained government agencies average about 49 months to order, acquire, and install new computer systems vs. about 9 months in the private sector. Criminals can purchase state-of-the-art technology as soon as it becomes available (Webster and de Borchgrave 1998).

Cybercrime is ra*mpant, with the increase rate higher than the increase rate of deterrence*

The enormous and exponentially growing capacities for electronic storage, transmission and rapid manipulation of binary data changed the modern landscape virtually overnight (Fraser 2003).

Engineering for ease of use is not being matched by engineering for ease of secure administration. The gap between the knowledge needed to operate a system and that needed to keep it secure is resulting in increasing numbers of vulnerable systems (Allen 2001).

The rapid quantitative increase in the criminality and its qualitative changes, caused by the aggravation of contradictions indifferent regions of public life, by the frequent reorganisations of the system of law-enforcement agencies, the imperfection of legislation and its frequent change, contribute to the acceleration of the process of the development of computer criminality as social phenomenon.

People call for making the punishment fit the cybercrime (Vamosi 2003), but how? Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk on the Net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations' security. Headlines of cyber attacks command our attention with increasing frequency (McConnell International LLC. 2000).

Although several countries, particularly in Europe and Asia, were found to have addressed a number of these broader information security factors, few countries were able to demonstrate that adequate legal measures had been taken to ensure that perpetrators of cyber crime would be held accountable for their actions (McConnell International LLC. 2000).

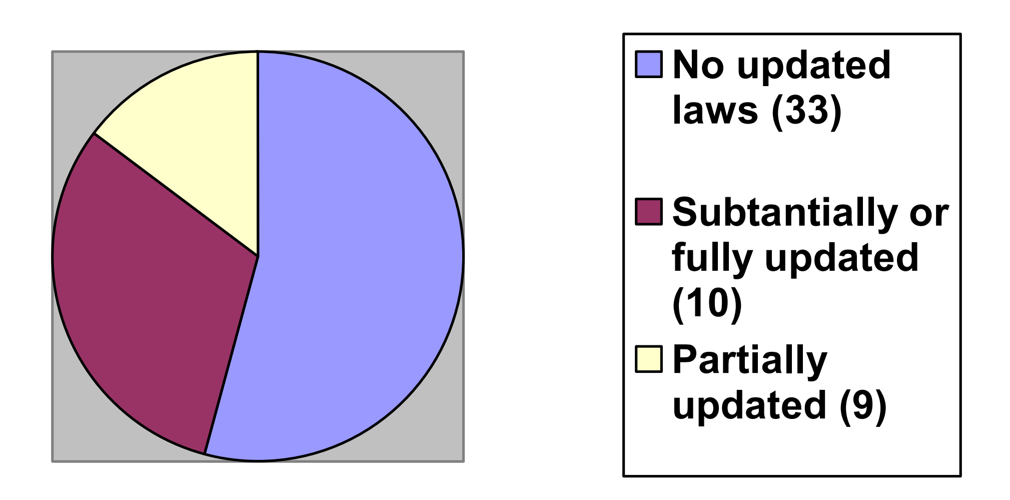


Figure 8 Extent of progress on updating cybercrime laws

Source: McConnell International LLC. 2000.

Figure 8 provides a categorization of the 52 countries surveyed. The laws of most countries do not clearly prohibit cyber crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their “virtual” counterparts. According to the principle of “nullum crimen sine lege, mulla poena sine lege,” lacking of law punishing cybercrime sets up the deterrent probability at zero, while the actual punishment is also zero. Then, the expected utility of the offender equals the utility when he or she is undetected.

Even if there is such law, effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes (McConnell International LLC. 2000).

The development of cybercrime necessitates the updating of law. For instance, six weeks after the Love Bug attack, the Philippines outlawed most computer crimes as part of a comprehensive e-commerce statute (McConnell International LLC. 2000).

Factors influencing the severity of punishment against cybercrime

As the conclusions of McConnell International LLC. (2000), weak penalties

limit deterrence. Why does creating a virus carry lighter penalties than marijuana offences? (McCullagh 2004). The possible answer from economists will be related to the elasticity of these two kinds of crime. Unlike the marijuana offences that are inelastic, cybercrime is more elastic. Tougher punishment for drug crime will be less effective than for cybercrime. But considering the marginal deterrence, when the punishment is too light for cybercrime, it certainly does not deter, either. Lack of certain degree of severity, punishment will not prevent potential criminals from committing crimes they are planning, because even if they are probably captured, their expected benefit is still higher than expected cost. It is the marginal deterrence of the punishment but not the elasticity of the crime is working.

There is a good excuse for capital punishment from the viewpoint of law and economics, saying that some countries are relatively poor and probably cannot afford to invest on detecting criminals, lengthy convicting and sentencing, and enforcing the imprisonment sentence. Therefore, capital punishment is still reserved in many countries, and is being further extended to cybercrime.

Principally, capital punishment cannot be applied to the specific cybercrime provided in Chinese criminal law (Articles 285, 286). However, capital punishment can be applied to the previous offences utilizing computer information systems, e,g. offence of financial fraud, theft, embezzlement, theft of national secret, and other offences (Article 287). If criminals are rational, they will respond to increases in the expected value of punishment by reducing their criminal activity. Even if they are driven by irrational factors, as long as they react rationally, at the margin of their activity, this response will follow (Garoupa 2003).

However, at the same time, some methods adopted in some countries cannot completely explained by the above theory. Take the example of

applying long-term imprisonment to the offences with low detection probability. The expense of the long-term imprisonment is quite huge. Then, it may be said that under these circumstances, the governmental investment is insufficient, while the emphasis is put on execution, the detection is ignored. This is related to the value orientation of the government.

Some countries completely breach the rational choice. They seem to be hard to afford for detection, conviction and execution, while on the other hand they established cyber police, employing huge police forces. The tasks of these cyber police include detection and evidence collection, as well as cybercrime prevention with techniques and human resources, forming a "cyber information dam". The expense is also huge.

In these countries, the concerns on privacy of individuals abdicate to the national security and social order. It proves that, in the information age, the public organs get increasingly greater power of surveillance and interception. Since 1990s, the world is frequently attacked by the terrorists, individuals' individualism is gradually submerged by the voice of national interests and international co-operation. The role of punishment in the deterrence of crime is undoubtedly unearthed. Whether in poor or wealthy countries, the severe punishment is being used universally to cybercrime. This can be explained as decreasing the expected benefits of cybercrime while increasing the expected costs, forcing the offenders to give up committing the offences and to choose legal activities. This implicates that the means the modern countries take to decrease crime are direct prevention, plus increasing detection probability and increasing punishment severity.

However, the following factors deserve further consideration:

1. Whether the information dam is effective? The filtering and

blocking of information is expensive and ineffective. As the substitute of severe punishment, it is either the necessary waste of democracy (compared with over-criminalization), or the necessary limit to democracy (compared with information freedom). Private deterrence effort might fail as public deterrence increases. Individuals might be less vigilant about crime if they felt the authorities had it under control. Firms should secure their networked information. Governments should assure that their laws apply to cyber crimes. Firms, governments, and civil society should work cooperatively to strengthen legal frameworks for cyber security (McConnell International LLC. 2000).

2. Whether the severe punishment is cheap? There have been hundreds of studies done concerning the cost of the death penalty, proving that the death sentence is not only expensive but also easy to execute the innocent. The cost of imprisonment is also high. Because the cost of severe punishment costs differently in different countries, the legislature and the law enforcement have the different tendency in implement different severity of punishments, which can bring about further jurisdictional problems.

3. Whether the severe punishment is effective? Imposition of severe punishment on light offence has the effect of inciting serious offence. Some crime could be displaced to another offence type, time or location. If criminals have target incomes, deterrence could imply that more crime would occur, for example, there could be more attempted break-ins that the police managed to halt. The deterrence of established criminals could encourage the entry of replacements into the crime industry. Given that the detection probability is very low, and there is no way to increase it, the severe punishment again meets the limitation. It turns out that the severe punishment does not work. According to the formulation, when $p=0$, the expected utility of the offender equals the utility when he or she is

undetected. So, the severe punishment to some extent needs the support of the detection probability. Or else it loses any foundation on which it exists. The punishment delivers no deterrence at all.

Conclusion

Although people are sure that poor information security reduces the competitiveness of nations (McConnell International LLC. 2000), as yet there is no mechanism as perfect as to eliminate this negative externality of information economy. The co-existence of various mechanisms inevitably causes conflicts and wastes. The result of the economic analysis of the punishment on cybercrime seems to destroy all hypotheses. However, the society does not shrivel. The coordinative framework of the cyberspace needs the coordinative countermeasures of the society. Even if the cost is high, the success rate is low, after hard game, the balance between crime and punishment will be reached at last.

References

1. Adams, J., 1996. Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet, Computer and High Technology Law Journal, 403 (1996).
2. Adreano, Siegfried (eds), 1980. The Economics of Crime (Wiley and Sons, New York, 1980).

3. Allen, J., 2001. CERT System and Network Security Practices (2001). http://www.cert.org/archive/pdf/NCISSE_practices.pdf.
4. American Society for Industrial Security, Cybercrime-fighting Tools Still Lacking, Security Management, 40 (May 2004).
5. Beccaria, C., 1774. An Essay on Crimes and Punishment.
6. Becker, Gary S., 1968. Crime and Punishment: An Economic Approach, Journal of Political Economy, 169-217.
7. Behar, R., 1997. Who's Reading Your E-mail? Fortune, 66 (3 Feb. 1997).
8. Bentham, J., 1789. An Introduction to the Principles of Morals and Legislation.
9. Blackstone, W., 1765-1769. Commentaries on the Laws of England, A Facsimile Edition of the First Edition of 1765–1769.
10. Carter, D., 1995. Computer Crime Categories: How Techno-Criminals Operate, 64 FBI Law Enforcement Bulletin, 21 (July 1995).
11. Commission of the European Communities, 2000. Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime, COM (2000) 890, final.
12. Computer Security Devision, Computer Security Resource Center, National University of Standards and Technology, 1993. Clipper Chip Technology, in Encryption Key Recovery, 30 April 1993. http://csrc.nist.gov/keyrecovery/clip.txt
13. CSI/FBI, 2000. Computer Crime and Security Survey (2000). http://www.pbs.org/wgbh/pages/frontline/shows/hackers/risks/csi-fbi2000.pdf.

14. CSI/FBI, 2005. Computer Crime and Security Survey, Computer Security Institute, 2005.

15. Davidson, Alistair, 2003. Decentralization, Disease and Terorism, 14 April 2003. http://www.eclicktick.com/decentralization__disease_and_terrorism__.htm

16. Department of Treasury Office of Tax Policy, 1996. Selected Tax Policy Implications of Global Electronic Commerce, November 1996.

17. Dizard, Wilson, 1982. The coming information age: an overview of technology, economics, and politics, New York: Longman.

18. Dnes, Antony W., 1996. The Economics of Law, Oxford: International Thomson Business Press, 1996.

19. Ehrlich, I., 1973. Participation in Illegitimate Activities: A Theoretical and Empirical Investigation, 81 Journal of Political Economy 521.

20. Ehrlich, I., 1975. The Deterrent Effect of Capital Punishment: A Question of Life and Death, 65 American Economics Review 397.

21. Ehrlich, I. and Mark, R., 1977. Fear of Deterrence: A Critical Evaluation of the "Report of the Panel on Research on Deterrent and Incapacitation Effects," 6 Journal of Legal Studies 293.

22. Fields G., 2004. Cyberexperts and Engineers Wanted by FBI, Wall Street Journal, B1 (6 April 2004).

23. Findlay, 1999. The Globalisation of Crime (Cambridge University Press, 1999) pp.138-166.

24. Fraser, B. T., 2003. Welcome to Computer Crime Research Resources. http://mailer.fsu.edu/~btf1553/ccrr/welcome.htm (last visited 15 Aug. 2003).

25. Garg, A., Curtis, J. and Halper, H., 2003. Quantifying the Financial Impact of IT Security Breaches, Information Management and Security (11) 2, 2003, 74-83.

26. Garoupa, Nuno, 2003. An Economic Analysis of Criminal Law, Oct. 2003. http://esnie.u-paris10.fr/pdf/textes_2004/Garoupa_criminalaw01.pdf.

27. Gelbstein, E., and Kamal, A., 2002. Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security, the United Nations ICT Task Force and the United Nations Institute for Training and Research (2nd ed., 2002).

28. Hale, C., 2002. Cybercrime: Facts and Figures Concerning the Global Dilemma, Crime and Justice International, Vol. 18, No. 65.

29. Harris, J.R., 1970. On the Economics of Law and Order, 78 Journal of Political Economy 165.

30. Hatcher, M. et al., 1999. Computer Crimes, 36 AM. CRIM. L. REV. 397 (1999)

31. Hellmann, 1980. The Economics of Crime (St. Martin's Press, New York, 1980).

32. IMF, 2002. Global Financial Stability Report, A Quaterly on Market Developments and Issues, June 2002, International Monetary Fund.

33. Institute for Security Technology Studies (ISTS), 2002. Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment (2002).

34. Kingdon, John, 1994. Shooting the Messenger: The Liability of Internet Service Providers for Prohibited Expression, 1994. http://www.catalaw.com/logic/docs/jk-isps.htm

35. Koch, L. Z., 2000. Open Sources Preventing Cybercrime, Inter@ctive

Week, 34 (10 July 2000).

36. Lee, M. et al., 1998. Comment, Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal, 14 Berkeley Technological Law Journal 839, 844 (1998).

37. Lenk, K., 1997. The Challenge of Cyberspatial Forms of Human Interaction to Territorial Governance and Policing, The Governance of Cyberspace (Routledge, New York, 1997).

38. Levitt, Steven D., 2005. "The Economics of Crime and the Criminal Justice System." NBER Website. 1 Sept. 2005. at http://www.nber.org/reporter/fall98/levitt_fall98.html.

39. Loeb, M. P., 2004. The True Cost of Cybercrime, Network Computing, 69 (1 April 2004).

40. Longstaff, T. A., 1999. International Coordination for Cyber Crime and Terrorism in the 21st Century, presentation at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Hoover Institution, Stanford University, Stanford, California (6-7 Dec. 1999).

41. Lukasik, S. J., 2000. Protecting the Global Information Commons, Telecommunication Policy, (24)6-7, 2000, 519-531.

42. Mardesich, J., 1996. Laws Across the Country Become Relevant in Connected World; Jurisdiction at Issue in Net Legal Cases, San Jose Mercury News, 1E (8 Oct. 1996).

43. McAfee, 2005. McAfee Virtual Criminology Report: North American Study into Organized Crime and the Intertnet, July 2005. http://www.mcafeesecurity.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf.

44. McConnell International LLC., 2000. Cyber Crime . . . and

Punishment? Archaic Laws Threaten Global Information: Archaic Laws Threaten Global Information, Dec. 2000. http://www.witsa.org/papers/McConnell-cybercrime.pdf.

45. McCullagh, Declan, 2004. Punishment fails to fit the cybercrime, ZDNet UK, 19 Aug. 2004. http://www.crime-research.org/news/19.08.2004/574/

46. McKenna, B., 2003. UK Police Promise Charter to Guard Good Names, Computers and Security, vol. 22, issue 1, 38-40.

47. Molander, R. C. et al., 1996. Strategic Information Warfare: A New Face of War, xiii (1996). http://www.rand.org/publications/MR/MR661/.

48. Morris, D. A., 2001. Tracking a Computer Hacker, USA Bulletin (May 2001).

49. National Commission, 2004. On Terrorist Attacks upon the United States, 9/11 Commission report, August 2004. http://www.9-11commission.gov/report/911Report.pdf.

50. National Police Agency, 1998. Keisatsu Hakusho, Haiteku Hanzai no Genjo to Keisatsu no Torikumi (Japan Police White Paper, The Situation of High-tech Crime and the Suppression of Police).

51. O'Connor, R. J., 1997. Computers Vulnerable to Insiders, San Jose Mercury News, 3C (6 March 1997).

52. Park, E., 2004. Analysis of Internet Crime in Korea and Countermeasures. http://www.iap.nl.com/speeches2/internetcrime.html (last visited 23 July 2004).

53. Parker, D. B., and Nycum, S. H., 1984. Computer Crime, Communication of the ACM, vol. 27, no. 4, 313-315 (April 1984).

54. Peters, A., 1971. Computers and Society: A Course, IIT, 30-38, (1971).
55. Philip, A. R., 2002. The Legal System and Ethics in Information Security (15 July 2002). http://www.sans.org/rr/papers/31/54.pdf.
56. Rahul Telang, Sunil Wattal (2005), Impact of Vulnerability Disclosure on Market Value of Software Vendors: An Empirical Analysis, 4th Workshop on Economics and Information Security, Boston, 1-3 June. http://infosecon.net/workshop/pdf/telang_wattal.pdf.
57. Ramo, J. C., 1996. Crime Online: Mobsters Around the World are Wiring for the Future, Time Digital, 32 (23 Sept. 1996).
58. Rottenberg (ed), 1973. The Economics of Crime and Punishment (American Enterprise Institute for Public Policy Research, Washington (DC), 1973).
59. Roush, W., 1995. Hackers: Taking a Bite Out of Computer Crime, Technology Review, 32 (April 1995).
60. Salgado, R. P., 2001. Working with Victims of Computer Network Hacks, USA Bulletin (March 2001). http://www.cybercrime.gov/usamarch2001_6.htm.
61. Sofaer, A. D. et al., 2000. A Proposal for an International Convention on Cyber Crime and Terrorism (Harvard, 2000).
62. Speer, D. L., 2000. Redefining borders: The Challenges of Cybercrime, Crime, Law and Social Change 34, 259-273 (2000).
63. Stanley, Timothy Jamesm, 1995. Optimal Penalties for Concealment of Crime, 22 December 1995.
64. Stigler, G.J., 1970. The Optimum Enforcement of Laws, 78 Journal of Political Economy 526.

65. Stoll, C., 1988. Stalking the Wily Hacker, Communication of the ACM, vol. 31, no. 5, 484-497 (May 1988).

66. Sullivan (1973. The Economics of Crime: An Introduction to the Literature, 19 Crime and Delinquency, 138-149.

67. Tullock, G., 1967. The Welfare Costs of Tariffs, Monopolies and Theft, Western Economic Journal 5, 224-232.

68. Ullman, R., and Ferrera, D., 1998. Crime on the Internet, Boston Bar Journal, Nov./Dec. 1998, No.6.

69. Vamosi, Robert, 2003. Make the punishment fit the cybercrime, 10 Sept. 2003, CNET Reviews. http://reviews.cnet.com/4520-3513_7-5073597.html.

70. Webster, W. H., and de Borchgrave, 1998. A. Foreword, in Peterson, Gallagher, Borchgraze, Cillusso, S. Lanz (ed.), Berkowitz (ed.), William H. Webster, Center for Strategic and International Studies, Cybercrime... Cyberterrorism... Cyberwarfare... (Nov. 1998. http://www.csis.org/pubs/cyberfor.html.

71. Wolf, J. B., 2000. War Games Meets the Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money, American Journal of Criminal Law, Vol. 28, 95-117.

CHAPTER XI CONCLUSIONS

The current information systems are insecure systems, while the present Internet is an insecure network. Cyberspace can be considered as the expansion of society, while cybercrime is the extension of criminal phenomena. Although cyberspace is not entirely independent, there is the possibility and even necessity for autonomy within the independent factors. Technicians are constantly inventing technological countermeasures to deal with issues of cybersecurity, but an increasing number of commentators argue that the techniques of security cannot keep pace with techniques for discovering loopholes in information systems and for launching attacks on information systems. It is impracticable to solve the whole problem merely by the means of technology.

To some extent, cybercrime mobilizes law. Criminal law and other laws, professional codes, industrial self-discipline and user ethics form guidelines, though their functions are quite varied as between the different countries. Most of the modern democratic countries do not exploit penalties as primary means for correcting human behaviour. Criminal law remains the main tool. However, if criminal law cannot respond to the reality of crime, if law cannot be enacted to impose a suitable liability on harmful activities, and if law cannot be enforced by

qualified personnel, the law will unquestionably be ineffective. In fact, in the current technological environment, legislature and law enforcement can hardly adjust their activities in response to the new situations. Criminal law becomes a law the principle and stability of which hamper its inherent functions.

Law-enforcement agencies have found that it is much more complex to detect, investigate, and convict cybercriminals than traditional criminals. In the networked world, it has become increasingly uncomplicated for criminals to avoid conviction by acting from a country where a conduct is neither criminalized nor prosecuted. International cooperation and legal harmonization are necessary for reducing investigation costs and increase enforcement effects.

As we mentioned above, the insufficiency of the existing legal framework and the inefficiency of detection and conviction imply that high costs will be involved in cybercriminal law enforcement. An inefficient and ineffective legal framework for control over cybercrime will run the risk of creating new unfairness in the information age. The deficiency of law and the prevalence of lawlessness may become two of the most notorious negative factors.

Neither laws nor technologies can do everything that people normally expect, even in their duties. The more appropriate strategies for the control of cybercrime require an arrangement of law enforcement, technological and market-based solutions.

